27.5.2020

Generic Framework for **Multi-Domain Federated ETSI GANA Knowledge Planes (KPs)** for **End-to-End Autonomic (Closed-Loop) Security Management & Control** for 5G Slices, Networks/Services

Automated and Self-Adaptive Security Policy Management & Control through Autonomics Software (powered by AI Models)

White Paper No.6 *produced under the umbrella of* ***ETSI PoC on 5G Network Slices Creation, Autonomic & Cognitive Management and E2E Orchestration; with Closed-Loop(Autonomic) Service Assurance of Network Slices; using the Smart Insurance IoT Use Case***

Edited by ETSI 5G PoC Consortium Steering Committee and Contributors
ETSI TC INT AFI WG 5G POC

Table of Contents

Other Related Complementary White Papers:

- ***White Paper No.1:*** *C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes*

- ***White Paper No.2:*** *ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON – ONAP Architecture*

- ***White Paper No.3:*** *Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds*

- ***White Paper No.4:*** *ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes*

- ***White Paper No.5:*** *Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation*

Executive Summary

Artificial Intelligence Models (AI Models) are enablers for advanced intelligence in the management and control operations now strongly required for the evolving and future networks such as 5G Networks. AI algorithms bring benefits to diverse aspects in development and deployment of AI exhibiting systems such as Autonomic (Closed-Loop) and Cognitive 5G networks and their associated Autonomic Management and Control systems. ETSI (European Telecommunications Standards Institute) TC (Technical Committee) INT/AFI Working Group (WG) has recently published the de-facto standard on the GANA (Generic Autonomic Networking Architecture) Reference Model—An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services in which AI plays a role in autonomic management and control of networks and services [2]. ETSI TC INT/AFI WG is running a PoC (Proof-Of-Concept) Program on ***5G Network Slices Creation, Autonomic & Cognitive Management & End-to-End (E2E) Orchestration; with Closed-Loop (Autonomic) Service Assurance of IoT 5G Slices (using Smart Insurance Use Case)***. One of the topics being addressed in the broader scope of the 5G PoC is the combined consideration of E2E Closed-Loop Service Assurance and Security Assurance for 5G Network Slices using the so-called ETSI GANA Knowledge Plane (KP) Platforms. ETSI TS 103 195-2[2] defines an Intelligent Management and Control Functional Block called GANA Knowledge Plane (KP) that is an integral part of Management and Control Systems for the network. A GANA KP Platform and provides for the space to implement complex AI powered network analytics functions that must be performed by interworking modules for autonomic (closed-loop) decision-making and execution called GANA Decision-making-Elements(DEs). The KP DEs run as software in the Knowledge Plane (KP) Platform and drive ***self-* operations such as self-adaptation, self-optimization, self-monitoring, self-protection and self-defense*** objectives for the network and services by programmatically (re)-configuring Managed Entities (MEs) in the network infrastructure through various means possible. The means to program MEs include NorthBound Interfaces available at the OSS (Operations Support Systems), Service Orchestrator, Domain Orchestrator, SDN (Software Defined Networking) controller, EMS/NMS (Element Management System/Network Management System), NFV (Network Functions Virtualization) Orchestrator, etc. KP DEs are powered by Artificial Intelligence (AI) algorithms such as Machine Learning (ML), Deep Learning (DL), computational intelligence, etc., such that they execute as AI models or components that embed AI Models [2] [5] [19] [17] [22].

ETSI TC INT/ AFI WG has established that E2E Autonomic (Closed-Loop) Service and Security Assurance shall be achievable through the *Federation of GANA Knowledge Planes (KPs)* that implement components for Autonomic Management and Control (AMC) intelligence for specific network segments and domains. The industry seeks such an E2E Federated Framework, and the ETSI GANA Framework enables to define and standardize such a framework. Autonomics by the GANA Knowledge Plane (KP) for a particular network segment/domain is complemented by lower level autonomics introduced in Network Elements/Functions(NEs/NFs) of the particular network segment under the responsibility of the KP, such that the KP policy-controls the lower level autonomics introduced in NEs/NFs. The E2E federation of KPs for the various network segments/domains and their policy-controlling of lower levels autonomics in the NEs/NFs of their respective network segments enable the complementary multi-layer autonomics. The complementary multi-layer autonomics and the federations of KP Platforms shall realize (achieve) Holistic Multi-Domain State Correlation and resources programming by the GANA KPs for the network segments/domains such as the Access, X-Haul (Fronthaul, Midhaul and Backhaul), and Core Networks, etc. While such an E2E Federation of KP Platforms for multiple network segments (as domains) has to be primarily considered within a single network operator administrative domain, the E2E Federation of KPs may be extended to even span multiple network operator or enterprise network administrative domains.

ETSI TC INT/AFI WG Specifications such as ETSI TR 103 404, ETSI TR 103 495, and ETSI TR 103 473 V1.1.2 provide the answer to the question of how to implement GANA-defined autonomic manager components (called autonomic functions, i.e. GANA DEs) that implement control-loops in physical network elements/functions (NEs/NFs) and in Virtualized Network Functions (VNFs). This includes answers to how to complement the NE/NF Level autonomic manager components with autonomic manager components defined to operate in the realm outside of NEs/NFs (the realm of management and control systems for particular network architectures), i.e. in the realm called the GANA Knowledge Plane (KP).

This white paper introduces the *Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services*. *Why "**Generic**"?* Because: the required Security Management-DEs of the framework can be innovated by any player with competence in autonomic security management and control for networks; security functions from various vendors can be used in the framework; the framework defines information that can be exchanged by KP Platforms in federated security management and control across domains. The

Generic Framework services as blueprint for the industry in implementing the paradigm of Autonomic Security Management and Control within a network segment domain and across multiple domains within a single Network Operator and across multiple Network Operator administrative domains. Today, there does not yet exist a *standardized Generic Framework* in the industry that fulfils the requirements described in this White Paper. Therefore, the Generic Framework proposed in this White Paper is candidate for standardization in ETSI, as the industry moves to maximize efforts to evolve Network Automation to Autonomic and Autonomous Networks of the Future. As demonstrated in this White Paper, the ETSI GANA Framework provides principles that guide implementers of ***Autonomic Security Management and Control Components*** to take into consideration in the interaction of such autonomic manager components with other ***Autonomic Management and Control components*** such as autonomic manager components for ***Autonomic Quality-of-Service(QoS) Management***, ***Autonomic Monitoring Management***, etc. That enables to implement various scenarios for collaborative AMC intelligence by the various AMC Components (i.e. GANA DEs), such as *Security requirements based Autonomic (dynamic) QoS Dynamic Provisioning*; *Security requirements driven adaptive(autonomic) monitoring and analytics of certain types of network traffic flows in the network*; *Security requirements based Autonomic (dynamic) Mobility Management, etc.*

The paper then presents Check Point (a Global Network Security Solutions Vendor/Supplier) Capabilities that enable to implement various aspects of the Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services.

This White Paper has been written to lay the groundwork for standardization work that could be launched in ETSI TC INT on Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services, as concluded at the end of this paper.

NOTE: Readers are encouraged to follow the developments on this topic in ETSI, and to download and read complementary *White Papers* of the ETSI 5G PoC, which are available and downloadable at: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals. The PoC Consortium is not "closed-consortium", and welcomes new members in the course of the PoC program duration, which goes beyond 2018/2019/2020 timeframe. Contact details are included at the end of this White Paper, for those interested in the PoC results or joining the Consortium.

1. Key Takeaways of the White Paper

The Key Takeaways of this White Paper are as follows:

- Summarized Descriptions of ETSI GANA Model's Cognitive Decision Elements (DEs) as AI Models for Autonomic Management & Control (AMC) of Network Resources, Parameters, Services, and Security
- Summarized Descriptions of ETSI GANA Model as Multi-Layer AI Reference Model for Implementing Autonomic Management & Control (AMC) of Networks and Services (including 5G Network Slices)
- Insights on AMC as the paradigm behind the autonomic (Closed-Loop) Security Management and Control capabilities required in 5G
- Description of the Generic Framework for Multi-Domain Federated GANA Knowledge Planes for E2E Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services, and the aspects of the Generic Framework that pertain to E2E Autonomic Security Management & Control across Multiple Domains (Network Segments)
- Why Security Analytics by the Knowledge Plane (KP) Security Management DE may need to dynamically trigger and program On-Demand Monitoring of certain Traffic in the Network, and the role of Passive Probing and Analytics of Traffic copied from the Network
- Security Functions Placement/Orchestration in 5G Networks and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics
- Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection and Threats Predictions
- Implementing *Self-Protection & Self-Defending Behaviors* for specific Network Segments/Domains by GANA Knowledge Plane Platforms, within Single Network Operator and across Multiple Network Operators
- Knowledge Plane (KP) driven "Open-Loop" and "Closed-Loop" (Autonomic) Service and Security Assurance for SDN Environments, with a desirable capability of the Security Management-DE and the Monitoring-DE of the KP in being

able to collaborate in triggering On-Demand Traffic Monitoring in the Network for Analytics of Suspected Traffic at any time as may be necessary

- The Concept of Real-Time Security Threats Repository that can be implemented as part of the so-called GANA ONIX (Overlay Network for Information eXchange) system of Federated Information Servers
- Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection (including Intrusions Detections and Violations Detections) and Threats Predictions
- Check Point (Network Security Solutions Vendor) Capabilities that help implement the GANA based Generic Framework for E2E Autonomic Security Management and Control
- Check Point Capabilities for Implementing the ONIX System's Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks, with Illustration of a Security Management-DE Implementation
- Overview on Check Point Capabilities on Security Functions for Telco-Clouds and 5G Network, Programmability, and How to integrate with GANA Knowledge Planes (KPs)
- How to use the Check Point Security Management Platform (R80) and Check Point CloudGuard Dome9 to implement GANA Knowledge Plane (KP) Security Management-DEs
- Implementing a GANA KP Level Security Management DE using the Check Point R80 Platform Environment and its Data Lake
- Conclusions on what should be targeted for Standardization of the Generic Framework for E2E Autonomic Security Management & Control for 5G Networks

NOTE: Network Operator Business Models, Network Equipment Vendor Business Models, Network Security Solutions Supplier Business Models, and ISV (Independent Software Vendors) Business Models and Business Models for other players of relevance to the ETSI 5G PoC are described in more detail in White Paper No.1 [5], White Paper No.2 [19], White Paper No.3 [17] and White Paper No.4[22].

2. ETSI GANA Model's Cognitive Decision Elements (DEs) as AI Models for Autonomic Management & Control (AMC) of Network Resources, Parameters, Services, and Security

2.1. ETSI GANA as Multi-Layer AI Reference Model for Implementing Autonomic Management & Control (AMC) of Networks and Services (including 5G Network Slices)

The ETSI GANA (Generic Autonomic Networking Architecture) Reference Model is an Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services standardized by ETSI [2]. The Figure 1 presents the snapshot of the ETSI GANA Reference Model and the aspect of Multi-Layer Autonomics' Cognitive Algorithms for Artificial Intelligence (AI) and the levels of abstractions of self-management functionality. Self-management functionality is a logic (component) that implements a control-loop as the core driver of the self-management behavior in terms of orchestration and/or (re)-configuration of entities that should be orchestrated, managed, and dynamically (re)-configured by the logic to meet certain objectives.

The GANA Knowledge Plane (see Figure 1) is an integral part of Management and Control Systems that provides for the space to implement complex AI-powered network analytics functions performed by interworking Modularized Autonomic Managers (called Decision-making Elements (DEs)) that run as software in the GANA Knowledge Plane platform. DEs drive *self-* operations such as self-adaptation, self-optimization, self-monitoring, self-protection and self-defense objectives* for the network and services by adaptively and programmatically (re)-configuring Managed Entities (MEs) in the network infrastructure through various means possible: e.g. through the NorthBound Interfaces available at the OSS (Operations Support System), Service Orchestrator, Domain Orchestrator, SDN controller, EMS/NMS, NFV Orchestrator, etc. The GANA Knowledge Plane

should view the various management and control systems, such as OSS/BSS (Business Support System), E2E Service Orchestrator, and SDN controller, NFV Orchestrator, collectively as data/info sources or events sources. This is because the GANA KP is supposed to be the center of consolidated knowledge about the network and intelligence for autonomic and cognitive management and control of the network infrastructure based on data and knowledge and events obtained from the various systems by the GANA Knowledge Plane. Also because Complex Event Processing (CEP) over events retrieved (received) from the various systems should be performed by the GANA Knowledge Plane as discussed in ETSI White Paper No.16 [1] and GANA Technical Specification [2]. And in turn, the GANA Knowledge Plane DEs may dynamically and selectively fire commands (thanks to the cognitive and analytics algorithms employed by the KP DEs) into any or some of the systems. This depends on the target systems the GANA KP DEs determine to be the means by which the DEs' should use in attempt to adaptively and intelligently instantiate, scale-in, scale-out or program the PNFs (Physical Network Functions) and VNFs (Virtual Network Functions) of the underlying network infrastructure. For example, the GANA Knowledge Plane can fire commands into the E2E Service Orchestrator in attempts to achieve analytics-driven orchestration, as may be determined by the Decision Elements (DEs) of the Knowledge Plane. Another possibility is that the KP could fire commands through the OSS (if an OSS is available and is a strategic target for use in (re)-configuring the network), or through the SDN Controller, etc., instead, or in combination to firing commands into the E2E Service Orchestrator. As such, the GANA Knowledge Plane is to be viewed as the "brain" for which implementers should design and implement advanced Autonomic/Cognitive Management & Control (AMC) DE Algorithms that can program network infrastructure via any of the systems available for that and according to the capabilities available on the systems' northbound interfaces. The GANA Knowledge Plane should be viewed as an Advanced Analytics Platform that also retrieves Health Scores Data, Monitoring/Telemetry Data, Topology and Configuration Data from the SDN Controllers for the Production Network and from NEs, and use the data in making the complex decisions in the Closed-Loop (Autonomic) Management and Control operations on the network infrastructure. Other inputs to the Knowledge Plane required for its autonomic operations (e.g. autonomic service assurance) include Service Definitions and any mappings to QoS (Quality of Service) Classes, SLA (Service Level Agreements) Definitions & Customer Identifiers Info/Data from the Service Fulfilment functions (e.g. OSS/BSS).

Looking more closely at Figure 1, the Knowledge Plane (KP) level autonomics is considered as the "Macro-level" autonomics (control-loops for dynamic adaptation of behavior and state), while autonomics introduced in the Network Elements/Functions (NEs/NFs) is considered as "Micro-level" autonomics.

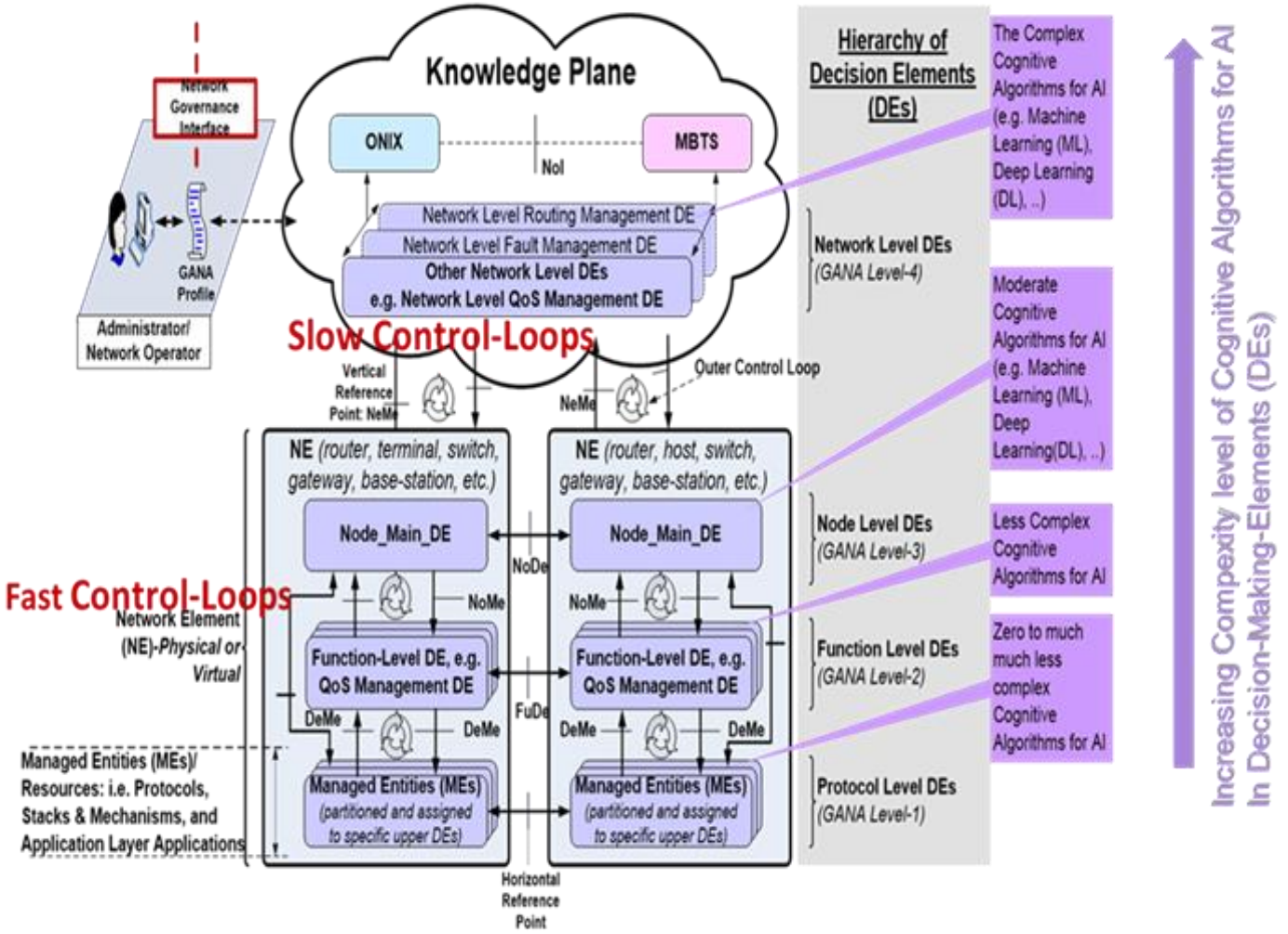

Figure 1: ***Snapshot of the GANA Reference Model and Autonomics Cognitive Algorithms for Artificial Intelligence (AI), and illustration of the notion of increasingly varying complexity of AI from within an NE up into the Knowledge Plane level***

The three key Functional Blocks of the GANA KP are summarized below (in reference to Figure 1):

- **GANA Network-Level DEs**: *Decision-making-Elements (DEs)* whose scope of input is network wide in implementing "slower control-loops" that perform policy control of lower level GANA DEs (for fast control-loops) instantiated in network nodes/elements. The Network Level DEs are meant to be designed to operate the outer closed control loops on the basis of "network-wide views" or state as input to the DEs' algorithms and logics for autonomic management and control (the "Macro-Level" autonomics). The Network-Level-DEs (Knowledge Plane DEs) can designed to run as a "micro services".
- **ONIX (Overlay Network for Information eXchange)** is a distributed scalable overlay system of federated information servers). The ONIX is useful for enabling auto-discovery of information/resources of an autonomic network via "publish/subscribe/query and find" mechanisms. DEs can make use of ONIX to discover information/context and entities (e.g. other DEs) in the network to enhance their decision-making capability. The ONIX itself does not have network management and control decision logic (as DEs are the ones that exhibit decision logic for Autonomic Management & Control (AMC)).
- **MBTS (Model-Based Translation Service)** which is an intermediation layer between the GANA KP DEs and the NEs ((Network Elements)—physical or virtual)) for translating technology specific and/or vendors' specific raw data onto a common data model for use by network level DEs, based on an accepted and shared information/data model. KP DEs can be programmed to communicate commands to NEs and process NE responses in a language that is agnostic to

vendor specific management protocols and technology specific management protocols that can be used to manage NEs and also policy-control their embedded "micro-level" autonomics. The MBTS translates DE commands and NE responses to the appropriate data model and communication methods understood on either side. The value the MBTS brings to network programmability is that it enables KP DEs designers to design DEs to talk a language that is agnostic to vendor specific management protocols, technology specific management protocols, and/or vendor specific data-models that can be used to manage and control NEs.

Remark: More detailed descriptions of the GANA Model are found in ETSI White Paper No.16 and in [5] [19] [17] and in the specification itself (ETSI TS 103 195-2).

According to the ETSI GANA Knowledge Plane (KP) concept, a Knowledge Plane (KP) Platform views various management and control systems such as SDN Controllers, OSS, Orchestrators, EMS's/NMS's and NFV MANO Components as event data sources and also as components or systems through which the Knowledge Plane can dynamically program the underlying network infrastructure. As illustrated on the figure below (Figure 2), other data sources may be used in implementing the Knowledge Plane. The figure illustrates the various kinds of APIs that may be required to integrate the ETSI GANA Knowledge Plane (KP) Platform with systems such as the following systems:

- OSS/BSS, Orchestrators,
- Production Network SDN Controllers,
- NMS/EMS,
- NFV MANO,
- SDN Controllers for OOB (Out-Of-Band) Monitoring Fabrics,
- Traffic Probing & Analytics Platforms,
- Telemetry Data Lakes,
- Big Data Analytics Apps,
- Ticketing Systems,
- other types of Info/Data/Event Sources that should feed the target GANA KP Platform with data, information, or events.

These aspects are further illustrated in Section 3.7 of this White Paper. ETSI TS 103 195-2[2] specifies APIs that should enable to integrate ETSI GANA Knowledge Plane (KP), SDN, NFV, E2E Orchestration, Big-Data driven analytics for AMC, and OSS/BSS systems (or configuration management systems in general). More details on this subject are found in [26] [19] [17]. [19] presents an approach to implementing a KP Platform using the ONAP open source software, and [19] also discusses how other open source products such as [9] [11] [12] [13] [14] [15] [16] can be used in implementing a KP Platform that integrates with other management and control systems depicted on Figure 2, such as SDN controllers, NFV MANO stacks, etc.

NOTE: In the case of the 3GPP 5G Architecture, functions such as the Network Data Analytics Function (NWDAF) [43] and the Management Data Analytics Service (MDAS) [44] should be integrated with the KP Platform so that KP DEs can use events and KPIs data from the functions in their autonomic operations. Sections 3.2 and 3.3 and Chapter 5 provide more detailed insights on this subject.

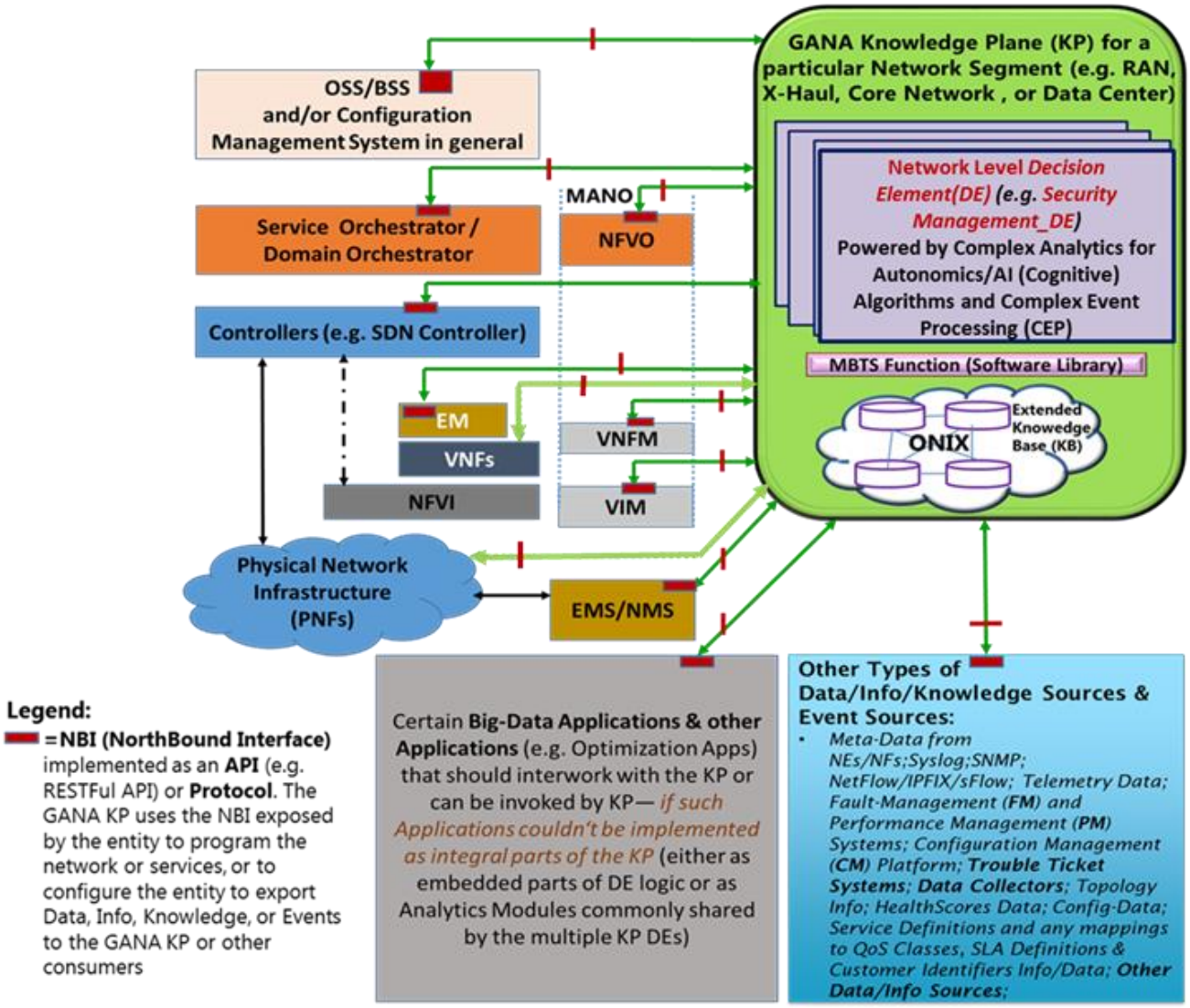

Figure 2: ***The Integration of the GANA Knowledge Plane (KP) with various management and control systems through which the Knowledge Plane can selectively program the network; and KP integration with Event Sources, Data Sources and Info/Knowledge Sources***

2.2. AMC as the paradigm behind the autonomic (Closed-Loop) Security Management and Control capabilities required in 5G

AMC shall help achieve End-to-End Closed-Loop (Autonomic) Security Management and Control in 5G E2E Architectures in the following way. The ETSI standard ETSI TS 103 195-2 [2], adopted by various SDOs/Fora in defining the AMC paradigm in the 5G Architectures, defines two levels at which an autonomic (closed-loop) manager for realising closed-loop security management and control can be instrumented (implemented) as a software module. In addition, such module should be powered by Artificial Intelligence (AI) algorithms such as Machine Learning (ML) or Deep Learning (DL) algorithms and other types of algorithms that enable it to intelligently achieve security assurance targets at the level of its operations scope. The autonomic manager component is referred to in the ETSI GANA Model as "**Security Management Decision-making Element(DE)**". The two levels for autonomics (control-loops) at which Security Management Decision-making Elements(DEs) can be designed to operate and made to interwork with each other as defined in ETSI TS 103 195-2 are called: (1) Network

Element/Function (NE/NF) level; and; (2) the realm of the outer management and control systems—the level of a part of management and control systems called the GANA Knowledge Plane (KP) Platform. Hence the two complementary DEs and levels for autonomic (closed-loop) security management and control operations are "NE/NF-Level **Security Management Decision-making Element(DE)"** and "**KP Level (also called Network –Level) Security Management Decision-making Element(DE)"**.

ETSI TS 103 195-2 defines the functionality of a Security Management-DE at NE/NF level and the functionality of a Security Management-DE at Knowledge Plane level (also called network level). A Security Management-DE is responsible for autonomically managing any security issues in the NE/NF or network, respectively. It does so by adaptively employing and managing Managed Entities (MEs) that pertain to the use of Certificates/Passwords Algorithms, Hash Algorithms, Encryption Algorithms, Access Control Mechanisms, Trust Mechanisms, Denial of Service (DoS) Detection/Prevention algorithms/mechanisms, Signature based intrusion detection mechanisms, and other security enforcement mechanisms. More details on functionalities expected of Security Management-DEs are found in ETSI TS 103 195-2.

The following figure (Figure 3) illustrates the two levels at which Security Management Decision-making Elements(DEs) can be designed to operate, with the higher level DE policy controlling the lower level DEs in NEs/NFs belonging to the network segment under the responsibility of the Knowledge Plane Level Security-Management-DE (the higher level DE). A Cognitive Security-Management-DE is one that has a capability of learning and reasoning, and so it is considered as a Deployable AI Model that needs to be tested before it is on boarded to run in a production environment. Both NE/NF-Level Security Management and the Network-Level Security Management-DE are expected to be cognitive and hence they need to be viewed as AI models. NE/NF-Level - embedded Cognitive DE(s) imply what can be called *"in-NE/NF" AI models*.

NOTE: Some Managed Entities (MEs) of an NE/NF that constitute part of the NE/NF resources, such as Protocols of the Stack, may have own intelligence for security enforcement or may intrinsically embed security features. However, the MEs communications with the outside world may need to be constrained or policy-controlled by the global security enforcement policies of the NE's Security Management-DE. And so the two GANA levels to give particular in designing and implementing autonomic (closed-loop) security management and control are the GANA Level 3 and Level 4.

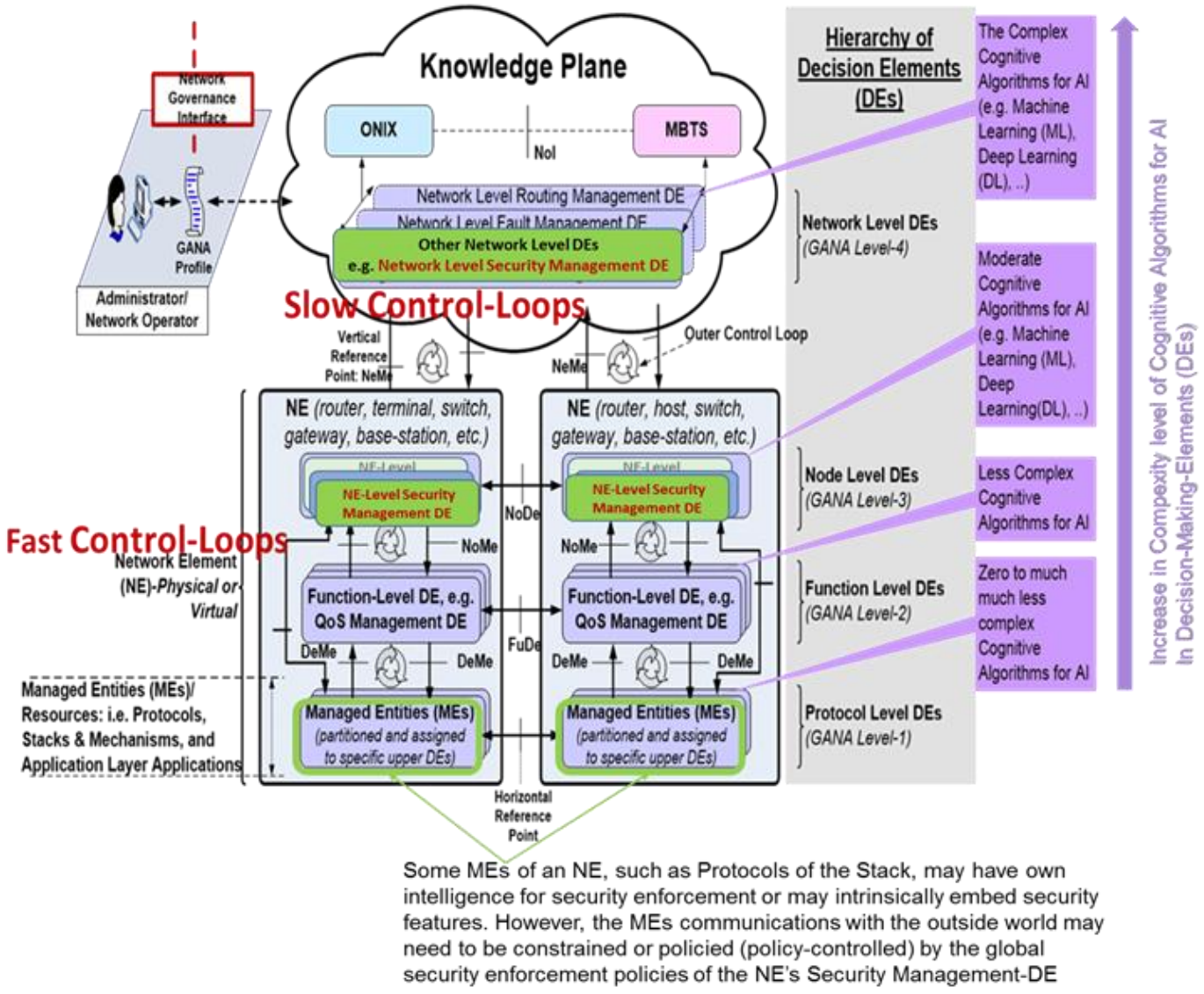

Figure 3: ***The two layers (abstraction levels) of Security-Management Decision-making Elements (DEs) that should be of focus in introducing Autonomic (Closed-Loop) Security Management and Control***

The Security-Management-DEs are expected to implement ***Self-Protection*** *and* ***Self-Defending*** *Policies and Operations* for specific Network Segments/Domains as driven by whole GANA Knowledge Plane (KP) Platforms within Single Network Operator and across Multiple Network Operators. Here we provide definitions of *Self-Protection* and *Self-Defense* behaviors that help implementers of Security-Management-DEs in implementing the DEs at the two GANA levels and make them to interwork:

- **Self-Protection** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically apply security policies and software patch updates that help protect the NE/NF and services using it from being compromised by security attacks (including intrusions, violations, etc.) and vulnerabilities/risks/threats (both, known and unknown attacks and vulnerabilities). While this low-level security enforcement on NE/NF level should be complemented (enhanced and controlled) by a capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at the network level dynamically computes and applies security policies for the whole

network (e.g. a specific network segment) and services using any knowledge of known attacks that may occur to NEs/NFs and network services, and applying software patches as may be necessary to protect the network resources from being compromised by attacks and any vulnerabilities.

- **Self-Defense** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically exercise the ability to detect security attacks (including intrusions, violations, etc.) and vulnerabilities(risks/threats) and apply security policies or software patch updates in reaction (defense) to any detected attacks or vulnerabilities/risks, and if the capability is more intelligent, then exercise the ability to predict security attacks and vulnerabilities and apply appropriate defense techniques. The effect of the self-defense actions is to minimize impacts of the detected or predicted attacks or vulnerabilities/risks/threats on services that depend on the NE/NF. As in the case of Self-Protection, the low-level security enforcement and security hardening on NE/NF level should be complemented (enhanced and controlled) by a capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at network level dynamically computes and applies security policies for the whole network (e.g. a specific network segment) and services using the knowledge of attacks or risks detected or predicted by a NE(s)/NF(s). In addition, applies software patches to defend and protect the network resources from being compromised by detected or predicted attacks or vulnerabilities/risks such that their impacts on network services is none or minimal. Self-Defense is closely related to the concept of **Resilience** (reactive and proactive resilience).

NOTE: The term *security* "***attack***" is generalized in this White Paper, to include all forms of security attacks or violations, including Denial of Service (DoS) Attacks for example, intrusions, and other forms of violations of the security of a system, service or network. There are various sources in literature that provide taxonomy on network, services and systems related security matters, e.g. [30].

A Security-Management-DE can be configured to operate in "Open-Loop Mode" or "Closed-Loop Mode". In Open-Loop Mode (allows human in the loop operation) the DE produces recommendations on actions the human operator can take to meet certain security enforcement or assurance objectives. ETSI TS 103 195-2 describes in much more detail these two modes of configuring a DE. The following aspects relate to how the autonomic security management and control part of the broader AMC is supposed to be realized by the interworking of the Security-Management-DEs hierarchically (at the two levels) and horizontally (for certain security management and control strategies and algorithms that may be implemented in a distributed fashion within and across NEs/NFs of network):

a) *Autonomics (closed-loop(s), i.e. control-loop(s)) operations by the NE-embedded Security-Management-DE*. As described in ETSI TS 103 195-2, the autonomics of this DE includes orchestration of security mechanisms/techniques within a Network Element (NE)/NF in order to achieve self-protection and self-defence for the NE/NF against security threats and attacks detected or predicted. Also the DE is responsible for planning and executing strategies for dynamically orchestrating various types of mechanisms/techniques for enforcing secure communications between the NE/NF and the outside world, e.g. firewalling of traffic, tunnelling of traffic (including dynamic VPNs provisioning to meet certain security objectives), encryption, use of trust models, etc.

b) *Autonomics (closed-loop(s), i.e. control-loop(s)) operations by the Knowledge Plane Level Security-Management-DE in the Knowledge Plane (Network Level Security-Management-DE)*. As described in ETSI TS 103 195-2, the autonomics of this DE includes Dynamic Security Policies computation and their enforcement by the Network Level Security Management DE of a Knowledge Plane (KP) onto the lower level Security-Management-DE of specific NEs/NFs. In addition, the DE's autonomics include dynamic programming of security-policy-enforcement components/functions such as SDN controllers and specialized security functions of the network such as Firewalls, Security Gateways, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). This is because the KP Level Security Management-DE is the DE responsible for the security assurance and self-protection and self-defence of the whole domain (network segment) against security attacks and threats. The KP Level Security-Management-DE should also exhibit intelligence (thanks to autonomics algorithms for achieving ***self-protection, self-healing, and self-defence*** for the network and its services) that causes the DE to dynamically orchestrate or (re)-configure security functions such as virtual firewalls, virtual IPSs, and virtual IDSs wherever they may be needed on demand in response to security threats detection and prediction. Such dynamic configurations by the KP level Security Management DE apply to physical security functions as well.

c) *Specialized Security Functions such as firewalls, IPSs, and IDSs, as Network Elements (NEs/NFs)* may need to embed the NE-embedded Security-Management-DE, like in the case of certain NEs/NFs such as routers and switches. In this way the DE can also serve as an embedded agent that should be policy controlled by the one at the KP level.

d) *E2E Autonomic (Closed-Loop) Security Management & Control in 5G* shall be achievable by way of Federation of the Knowledge Plane-Level Security-Management-DEs across multiple network segments/domains (RAN, X-Haul Transport, Core Network), following the principles for federated AMC outlined in the NGMN 5G E2E Architecture Framework [25]. According to the NGMN E2E 5G Architecture [25], E2E Autonomic (Closed-Loop) service assurance should be achievable through a federation of Knowledge Planes (KPs) that implement components for AMC intelligence for specific network segments (viewed as domains). According to the NGMN 5G E2E Architecture Framework [25], various types of common and generic information may be exchanged by federated KPs, and such information should include the following types of information:

- *Synchronization of actions across multiple KPs [ETSI TS 103 195-2]*: This is required, for example, to realize an effective E2E federation of Orchestrated Closed-Loop Security Management and Control (adaptive security enforcement and defense) in network infrastructure segments and across multiple domains (Technologically and/or administratively diverse domains). Examples of such domains are network segments (domains) such as Radio Access Network (RAN), X-Haul Transport Network (i.e. Fronthaul, Midhaul, Backhaul, etc.), "Multi-Access Edge Computing" (MEC) site or Core Network. E2E autonomic security management and Control should be achievable through a federation of KPs for the various network segments (domains) associated with a given E2E scope. In this case, each KP policy controls the AuFs (Autonomic Functions), meaning DEs, running in certain NEs/NFs within the network segment governed within the scope of the associated KP. The KP level AuF called the Security Management-DE implements the security policies for self-protection and self-defense of associated NEs/NFs and for securing a network zone under the responsibility of the DE, complemented by NE/NF level DEs required to realize 'fast control loops' within the NEs/NFs, in accordance with the generic autonomic networking principles [ETSI White Paper No.16].

- *Security event information (regarding a description of a detected security incident)*: An example is detected threats that may impact a peer domain, which could trigger an investigation of the detected threat that is identified by the collaborating KPs. The exchange of such security threats detection or predictions information may result in the KPs collaboratively negotiating an adaptation strategy (self-adaptation without human involvement) for adjusting security enforcement policies that each KP then applies to realize self-protection and self-defense for its associated network segment/ domain against the detected or predicted threat(s). For example, there may be some security threats detected in the access network domain by the KP for the access network that could have impact on X-Haul transport network domain as a peer domain or may have impact on the core network as the peer domain in terms of impact scope of the security threat(s).

- *Trust model (e.g. a reputation-based trust model) between the Autonomic Management and Control (AMC) administrative domains*: An example of such a trust model would be a kind of trust model that spans across autonomously managed and controlled domains, with the associated network infrastructure segments and their associated KPs, where each particular network segment has a KP.

- *Security related SLA (Service Level Agreement) violation detection*: The detection of an SLA violation, requires the associated KPs to initiate a resolution through a collaboration across the KPs to resolve the SLA discrepancies by reacting to resolve the detected discrepancies for an alignment with the configured SLA clauses in the SLA contracts that were established by the associated domain owners or stakeholders/partners

Remark: The Information that needs to be exchanged on a KP-to-KP Federation Reference Point, as well as the messages and communication means should be candidate for standardization (e.g. in ETSI TC INT AFI WG).

As illustrated on Figure 4, Security Modules in a Network Architecture are required at the three (3) hierarchical GANA Levels:

- GANA Knowledge Plane (KP) Platform level, by the Network Level Security Management -DE

- Node Level, by the Security-Management-DE at Node-Level (Network Element/Function Level), and this includes normal NEs and Layer4-Layer7 (L4-L7) Security Functions like IDS, IPS, Firewalls (FWs)
- Protocol Level (some security mechanisms may be intrinsically present in some protocols of the protocol stack of a Network Element/Function (NE/NF) or some protocols may have been designed to employ various security enforcement mechanisms/techniques in their operations)

Security modules implemented to operate in NEs/NFs are policy controlled by the Security-Management-DE operating as a Security Policy Engine in the associated GANA Knowledge Plane (KP) Platform. A GANA KP Platform enriches the Control Plane and the Management Plane as illustrated by the Integration of GANA KP with other management and control systems such as SDN Controllers, Orchestrators, OSS/BSS, MANO stacks, etc., as described earlier in this paper and in [22] [26].
On those levels the following module types/examples should be considered:

- **GANA KP Platform Level**: → Security API (Application Programming Interface) Library should be designed for the Security-Management-DE such that some inputs to the DE can be supplied through the API. And some specialized security Applications (runnable software) for addressing different aspects of security management and control can be developed such that they can be selectively invoked and managed by the Security-Management-DE. Such Applications may be developed to empower the Security Management-DE to offer "***Security-as-a-Service"*** (SaaS) for the various contexts addressed by the Applications. The Applications could be "composed" into "Security Services" that form a Service Container Library for the Security-Management-DE. The specialized security Applications that should be invoked and managed by the Security-Management-DE employ various security enforcement mechanisms/techniques such as encryption methods, tunneling management, authentication methods, etc.
- **GANA Node Level (i.e. Network Element/Function)**:→ A Network Element/Function of the type like a router or a switch should embed a Security-Management-DE as prescribed by the GANA principles, so as to implement a fast control-loop for self-protection and self-defense intelligence for the NE/NF. There are other types of NEs/NFs like L4-L7 security functions such as a Firewall, IDS, and IPS, that can be made to embed a Security-Management-DE to realize a fast control-loop for self-protection of the network and services the security function is meant to protect. And to some extent, the fast control-loop can also be meant for realizing self-defense of the NE/NF against certain attacks that may be aimed at rendering the NE/NF cease to function well. Some specialized Security Applications (runnable software) meant for addressing different aspects of security management and control can be developed such that they can be selectively invoked and managed by the Security-Management-DE. And such Applications may be developed to empower the Security Management-DE to offer "Security as a Service" for the various contexts addressed by the Applications that could be "composed" into "Security Services" that form a Service Container Library for the Security-Management-DE. The types of NEs/NFs that could offer "***Security-as-a-Service***" are L4-L7 types of NEs/NFs such as Firewall, IDS, IPS.
- **GANA Protocol Level or GANA Level 1 in general**: → At Protocol Level, some security mechanisms may be intrinsically present in some protocols of the stack of the NE/NF or some protocols may be designed to employ various security enforcement mechanisms/techniques in their operations. Other types of Managed Entities (MEs) at GANA level-1 may also embed security mechanisms or may be designed to employ various security enforcement mechanisms/techniques (e.g. encryption methods, tunneling management, authentication methods, etc.) in their operations. All the various security enforcement mechanisms/techniques that can be applied on a global scale within the NE/NF can be considered as forming a security enforcement mechanisms/techniques Library of the NE/NF. Such that the mechanisms/techniques can be orchestrated and employed by various entities within the NE/NF that require to employ them as required and enforced by the Security-Management-DE of the GANA Node(NE/NF).

NOTE: In the figure below (Figure 4), the security enforcement capabilities (e.g. mechanisms and logic) at GANA Level-1 and GANA Level-3 of an NE/NF may be activated in certain types of NEs/NFs of the network.

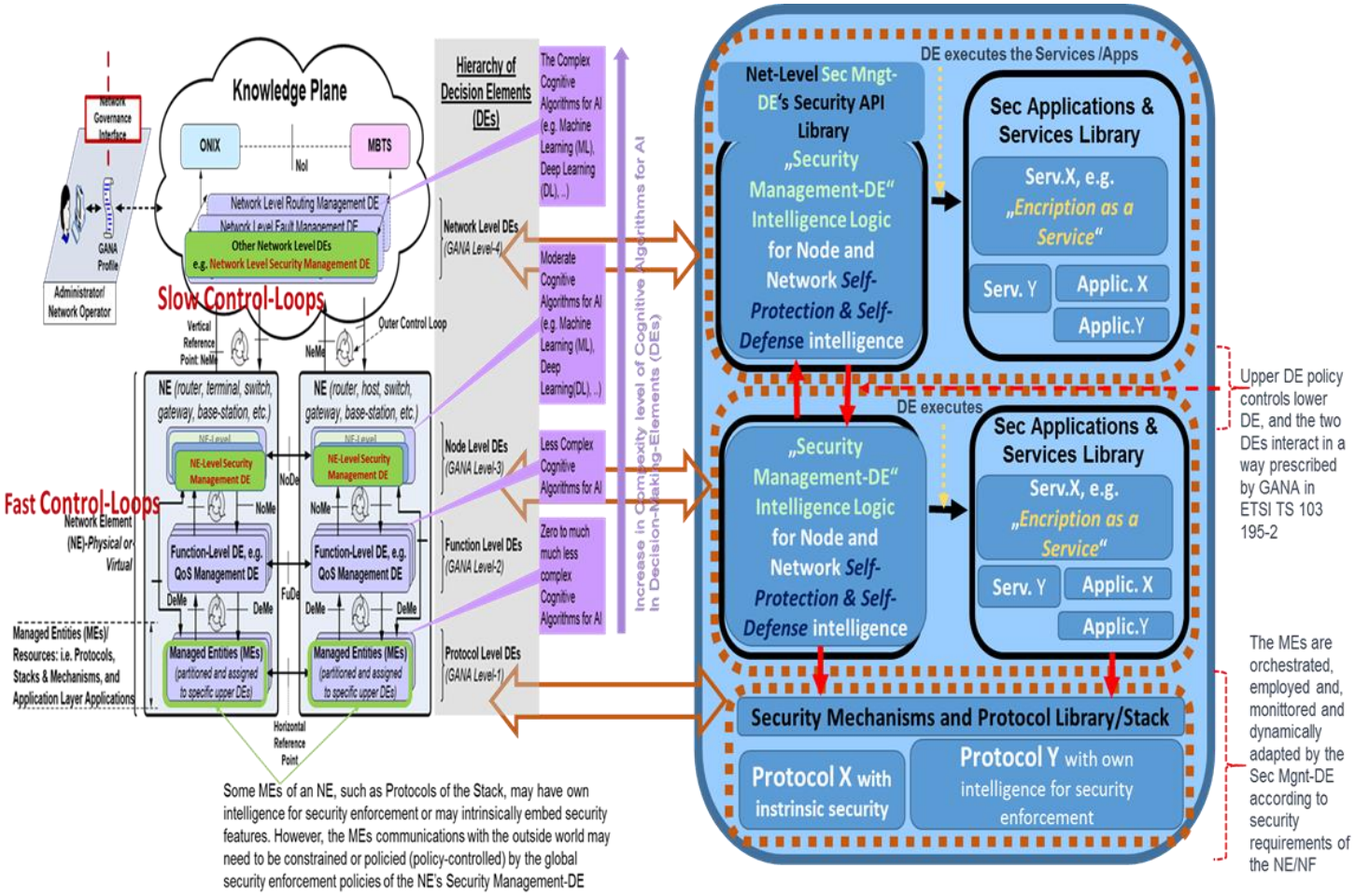

Figure 4: ***Hierarchical Security Management in GANA Framework***

The following diagram (Figure 5) provides an illustration of how a Network Level (KP Level) Security Management-DE can be implemented to drive autonomics control-loop over Security Functions as its Managed Entities (MEs) and dynamically program them to meet Self-Protection and Self-Defense Objectives of the network (e.g. as illustrated in [21] [23] [24]).

NOTE: The subject of *Self-Protection* and *Self-Defense* behaviors is further discussed later in Chapter 6.

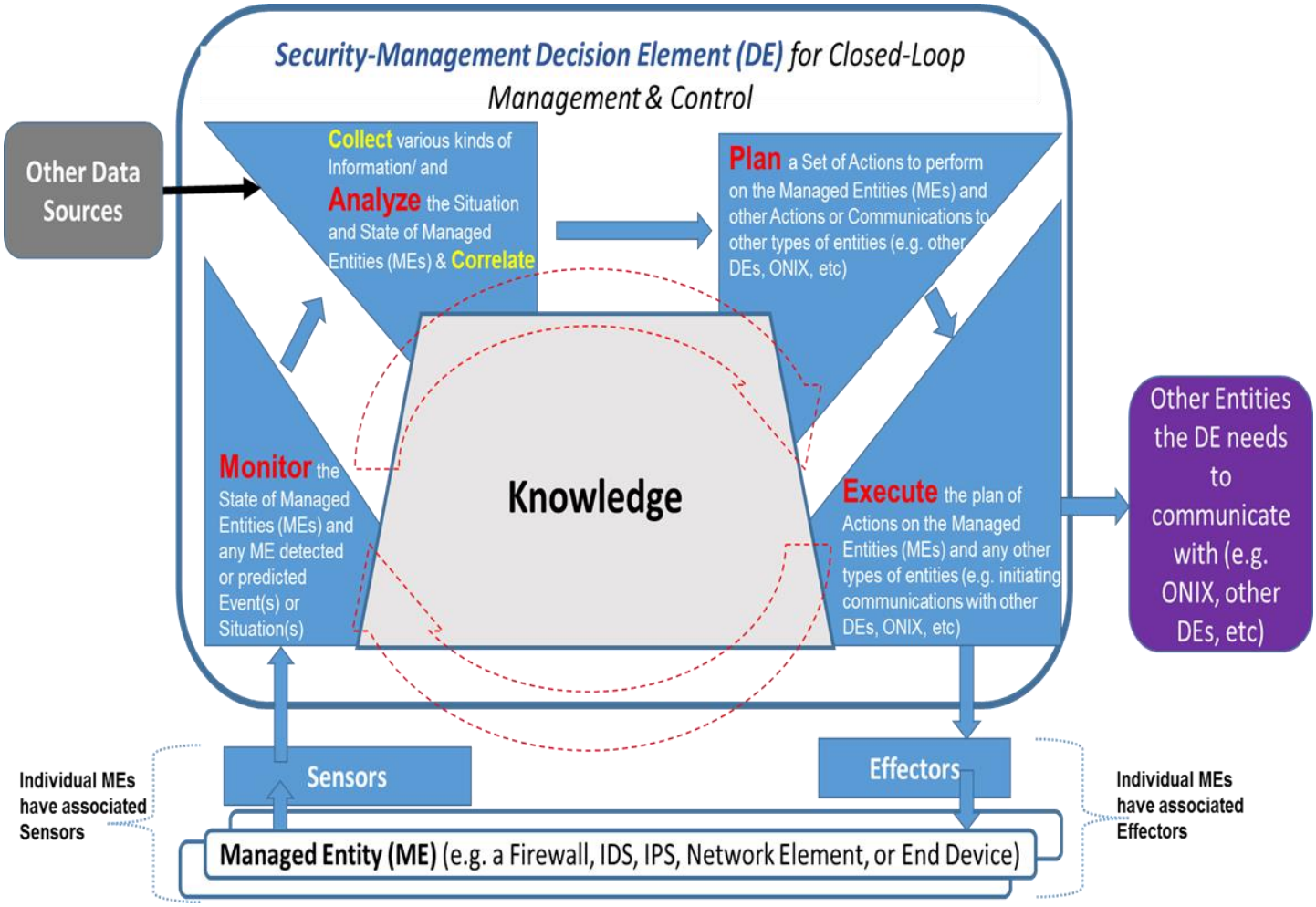

Figure 5: ***Illustration of how a KP Level GANA DE can be implemented (more details on approaches to designing GANA DEs are found in ETSI TS 103 195-2)***

2.3. Security Requirements that should be considered in the communications involving components for GANA AMC (i.e. DEs, MBTS, ONIX Services)

Another aspect of security in relation to AMC that needs to be considered in Autonomic Management and Control (AMC) operations by DEs relates to the following requirements:

- Identity Management for Autonomics components (e.g. DEs),
- application of Encryption mechanisms and protocols, and application of other mechanisms/techniques for securing DE to DE communications (as such communications should never be compromised), DE to ME (Managed Entity) communications, and for any other communications involving the enablers for AMC such as ONIX and its services.

2.3. Security Testing of Components for GANA AMC and their Services (i.e. DEs, MBTS, ONIX Services)

ETSI White Paper No.16 provides insights on the nature various potential suppliers of DEs as Software Modules/Components that can be loaded into NEs/NFs or into a GANA Knowledge Plane (KP) Platform. While Testing a Cognitive DE(s) like a Cognitive Security-Management-DE is about testing a deployable AI Model before the DE–Under-Test can be on-boarded into

the production environment, the functional and performance tests of the DE should be complemented by Security Testing of the DE against certain security requirements deemed necessary by the network operator (just like for any software modules). While Functional and Performance Tests for a Cognitive Security Management-DE is aimed at assessing the quality of decision-making capability, security tests of such a DE as a software module may involve the assessment of certain integration requirements for software components aimed at ensuring that the software component does not introduce security holes when on boarded into the production environment. [52] covers the subject of Testing AI Models and Testing GANA Functional Blocks.

3. The Generic Framework for Multi-Domain Federated GANA Knowledge Planes for E2E Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services

3.1. Overview

This chapter defines a Framework for guiding implementers in designing and implementing GANA Security Management DEs of the Knowledge Plane (KP) Platforms responsible for autonomic (closed-loop) security assurance of specific network segments/domains in the context of the E2E 5G Architecture. The framework also includes the enablers for achieving autonomic security assurance across multiple network operators (as collaborating domains) by way of federated Information sharing regarding security attacks and threats; as well as Orchestration and Programmability requirements for Security functions responsible for securing a network segment. In short, the Framework outlines the following aspects as part of what is desired of such a Framework:

- The Key Concepts
- The Aspects of the Generic Framework that pertain to E2E Autonomic Security Management & Control across Multiple Domains (Network Segments)
- Why it is desirable that Security Analytics by the Knowledge Plane (KP) Security Management DE can dynamically trigger and program On-Demand Monitoring of certain Traffic in the Network, and the role of Passive Probing and Analytics of Traffic copied from Network
- Security Functions Placement/Orchestration in 5G Networks and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics
- Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection (including Intrusion Detection or other forms of Violations Detection) and Threats Predictions
- Implementing *Self-Protection & Self-Defending Behaviors* for specific Network Segments/Domains by GANA Knowledge Plane Platforms, within Single Network Operator and across Multiple Network Operators

NOTE 1: Throughout these various aspects, this White Paper presents the Check Point Capabilities that enable to implement the requirements of the **Generic Framework**.

NOTE 2: The term *security* "***attack***" is generalized in this White Paper, to include all forms of security attacks or violations, including Denial of Service (DoS) Attacks for example, intrusions, and other forms of violations of the security of a system, service or network. There are various sources in literature that provide taxonomy on network, services and systems related security matters, e.g. [30].

3.2. Types of Network Security Challenges and 5G Slice-specific Security Issues of focus in this Framework, and the Core Architectural Principles for Autonomic Security Management and Control

5G network slices are associated with different Service Level Agreements (SLAs) and require strong isolation per slice so as to prevent threat propagations across network slices. The implication of network slicing is that slice specific security policies must be instantiated and applied for security assurance per slice.

In this section, we provide a summary of security challenges that we believe should be handled by way of automated security policies instantiations and installations at various points in network segments and at security perimeters between network segments or domains. Security challenges that should also be addressed by way of closed-loop (autonomic) monitoring for security attacks/threats, attacks/threats detection and predictions, autonomic planning of policies for adaptive security assurance and execution of actions that employ various methods for self-protection and self-defense for the network infrastructure and network services (including slices). NGMN has produced security requirements for 5G and continues to look into security challenges for 5G [4] [10]. European Union Agency for Network and Information Security (ENISA) published a "Threat assessment for the fifth generation of mobile telecommunications networks (5G)" [39]. [50] and [53] discuss the growing and strong requirement and call for Security Standards for 5G.

Efforts by the industry and research communities to capture such kinds of security challenges for 5G continue. For example, [47] discusses a recent survey on various security challenges for 5G (readers can read more on this survey in [47]), challenges such as the following aspects (not exhaustive, and we deduce that such challenges can be addressed through automated and autonomic security management and control) extracted from the White Paper by Heavy Reading [47]:

- *Security as a service (SECaaS) and the need for proactive security for known and unknown attacks*
- *Cloud RAN security, including fronthaul and backhaul security*
- *Core network signaling security*
- *5G Roaming network signaling security*
- *Areas and contexts of susceptibility to Fraud (calling for fraud detection then)*
- *Signaling protection against multi-protocol attacks*
- *The need to look into automating real-time security policy*
- *Need for visibility in RAN and core network by content inspection*

While some efforts have focused on looking at the security challenges that need particular focus on the RAN and core network, it is widely understood that there are various security challenges in other network segments such as the MEC edge, the X-Haul Transport Network and Data Centers, that have potential impact on other network segments, including RAN and core network. Therefore, there is a need for a holistic approach to correlation of attacks and threats, and the End-to-End (E2E) collaboration of security platforms that automate real-time security policy for the various segments (or domains). Hence the need for a "***Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services***".

There are other various sources that provide very valuable insights on security challenges in 5G, such as [4] [27] [10]. As another example of documented security challenges in 5G, a Table of security challenges in 5G (e.g. DoS attacks, signaling storms, configuration attacks, User identity theft, TCP level attacks, man-in-the-middle attacks, hijacking attacks, IMSI catching attacks, etc.) is presented in [28] and readers should read [28] for more details. There are many more sources worthy to consider on security challenges in 5G, e.g. [29] [37] [38] [39] [40] [41] [42] [45] [46].

The following diagram (Figure 6) illustrates two implementations Options for the interactions of a Security-Management-DE in the Knowledge Plane Level with a Security Function (e.g. Firewall, IPS, IDS, Security Gateway) or a Network Element/Function (NE/NF) in general that can be programmed for security enforcement objectives.
NOTE: The two options apply to the other DEs of the KP as well in their interactions with NEs/NFs, i.e. with or without the use of an MBTS function.

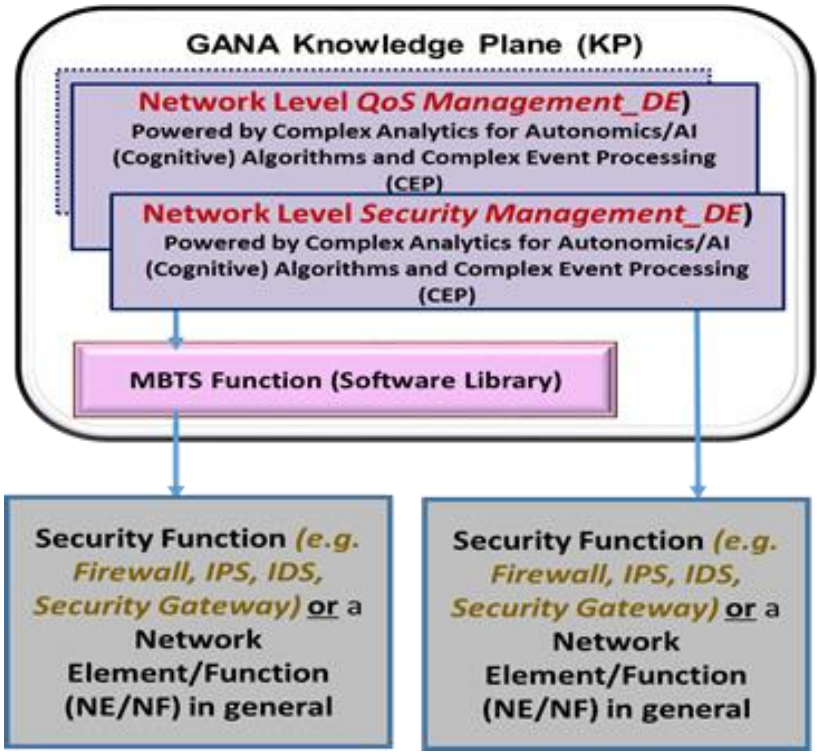

Figure 6: ***Two implementations Options for the interactions of a Security-Management-DE in the Knowledge Plane Level with a Security Function (e.g. Firewall, IPS, IDS, Security Gateway) or a Network Element/Function (NE/NF) in general***

With respect to the 3GPP 5G SBA (Service Based Architecture), the Network Level Security Management-DE in the Knowledge Plane (KP) Platform should also be connected to the GANA Node Level (i.e. the Node-Level (NF-Level)). Meaning it should be connected to a Security Management-DE that may be embedded (as a capability) within each node or be connected to an NF in general that does not embed a Security Management-DE. Such integration of the SBA functions (e.g. functions in the control plane) with the KP enables to achieve the following objectives:

- at least AMF (to know UE location and to manage UE mobility);
- SMF (to know traffic flow characteristics and to manage flows);
- UDM (to know which NF manage a UE, and manage UE subscription);
- PCF (to manage the policy);
- NRF (to know the load of each NF or a slice and manage NF selection);
- the user plane UPF (to detect certain anomalies such as traffic related anomalies).

The Network Level Security Management-DE in the Knowledge Plane (KP) Platform should also be connected to the NEF (to protect the NEF, which exposes services to an AF (Application Function) and to manage security protection with third party AFs).

[40] presents some examples of some insights on security requirements in the 5G SBA. Also, functions such as the Network Data Analytics Function (NWDAF) [43] [49] and the Management Data Analytics Service (MDAS) [44] should be integrated with the KP Platform for the core network so that events and KPIs data (results from analytics services) from the functions can be used by KP DEs in their autonomic operations (as discussed further in section 3.3). The KP Level Security Management-DE for the SBA Core Network can leverage the NWDAF's analytic services such as the observed service experience (which enables the Security Management-DE to be aware of traffic communications prediction). And so the KP Security Management-DE can also be aware of abnormal traffic behavior, and in case the UE causes a change in predicted traffic behavior or predicted location area, an AS (Application Server) could be notified. The KP DE needs to be aware of abnormal behavior related network data analytics services (communication related or mobility related), and such an event could be triggered to an Application

Server(AS) (any kind of third party server or MNO AS server) which subscribed to such an event through the NEF in case the AS is an OTT server. The AS could then request the PCF according to its rules of abnormal behavior to bar (delete temporarily a device) the UE (i.e. SIM) within the UDM(HSS) through the PCF. The KP may need to know of such dynamics in order to compute new decisions and plans of actions to execute.

In 5G, each network slice has its own security requirements and SLAs (Service Level Agreements) that need to be fulfilled. When a Network Slice has been orchestrated (w.r.t both an E2E Slice or a Slice within the scope of a specific network segment, e.g. RAN, X-Haul Transport, or Core Network), the security needs(policies) for the specific slice must be provisioned and the security requirements of the slice must be assured by autonomic means (closed-loop operations). The autonomic security assurance of the slice is meant to be achieved by the Security Management-DEs responsible for the security assurance of the slice during the lifetime of the slice. E2E autonomic security assurance of slices shall be achieved by way of federation of Security Management DEs across all the network segments as illustrated and described in the later sections of this white paper. What network slicing requires is that Security Management-DEs must be capable of fulfilling security requirements/needs of specific network slices. Network slice providers will desire to be able to select from the marketplace the appropriate Security Management-DEs software or whole Knowledge Plane (KP) platforms according to security requirements and SLAs that the Security Management DEs would be expected to fulfil when deployed for live operations. This is because Security Management-DEs capabilities and services may be different in terms of different level of security services they can provide (as discussed earlier on the subject of "Security Services" that form a Service Container Library for the Security-Management-DE). The following types of network slices have different security requirements/needs: network slice for defense industry, network slice for emergency services, network slice for Industry 4.0 vertical, network slice for Internet services, other types of network slices. This subject is covered in more detail in the later section on "Security Functions Placement in 5G Networks and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics".

The following diagram (Figure 7) illustrates the fact that in the GANA Knowledge Plane (KP) Platform, DEs interact in exchanging information/knowledge that enable the coordinating DEs to use the information in their decisions on (re)-configuring their respective Managed Entities (MEs)—which include the lower level DEs in NEs/NFs that are policy controlled by the KP DEs. The figure shows the Reference Point (Rfp) regarding DE-to-DE communications that may be necessary in some AMC objectives (with illustrations using ***Security-Management-DE***, ***QoS-Management-DE***, ***Routing-Management-DE***, *and* ***Forwarding-Management-DE***, *and* ***"other" network level DEs*** *such as* ***Fault-Management-DE***).

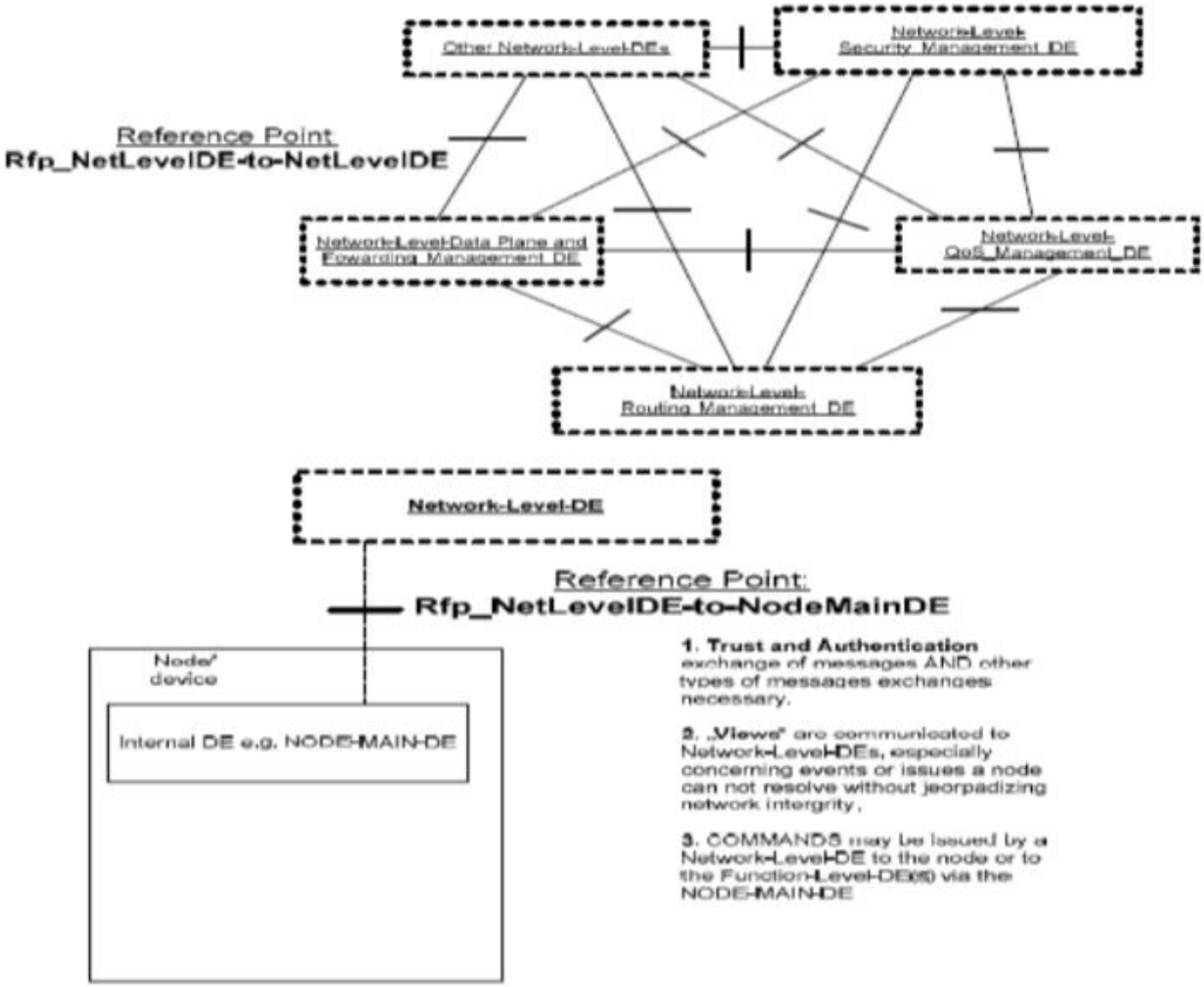

Figure 7: ***On KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on (re)-configuring their respective Managed Entities (MEs)***

Figure 8 presents elaboration on KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on dynamic/adaptive (re)-configuring their respective Managed Entities (MEs).

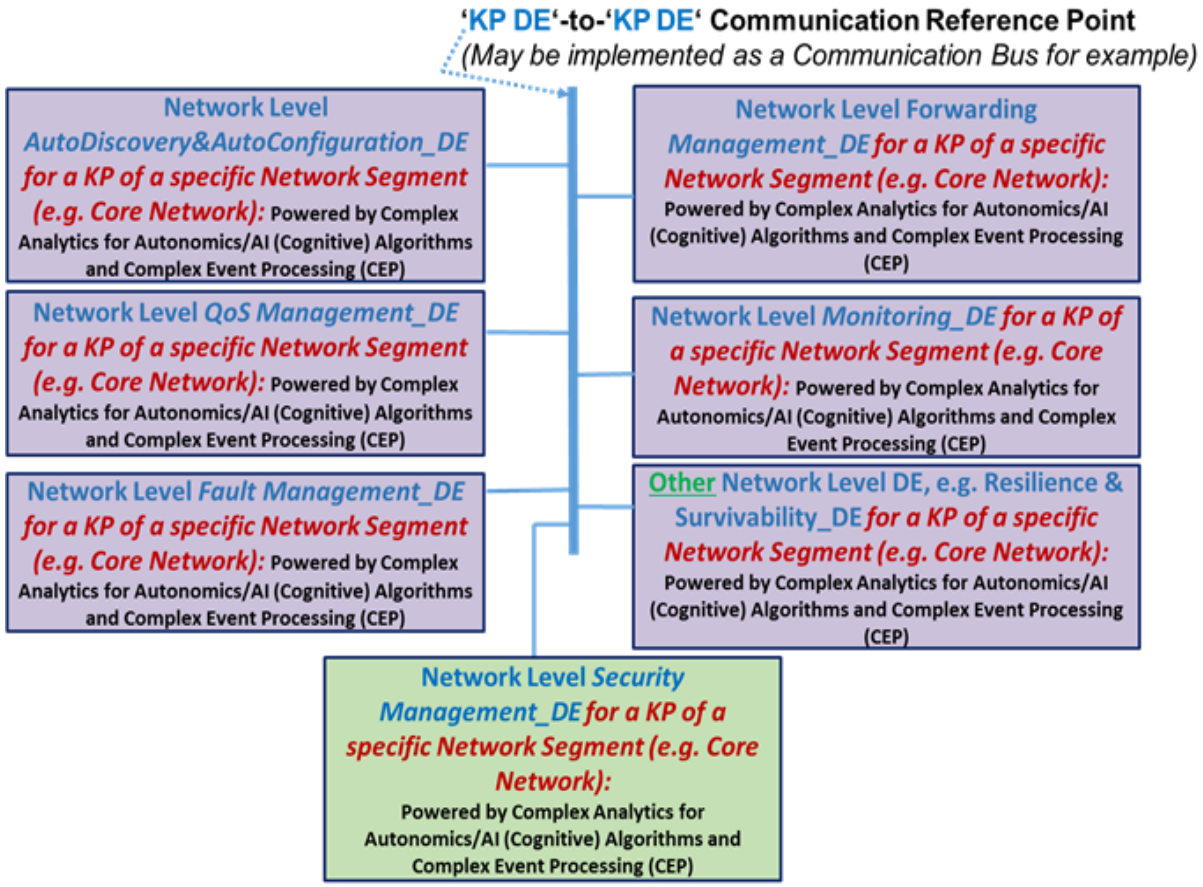

Figure 8: ***Elaboration on KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on adaptively (re)-configuring their respective Managed Entities (MEs)***

3.3. Integration of the GANA Knowledge Plane (KP) Platform for 5G Core Network with MDAS(MDAF) and NWDAF(NWDAS) Functions/Services, and how KP Security Management-DE can benefit from the Analytics Services of the Functions/Services

In brief, MDAF (MDAS) [44] and/or NWDAF (NWDAS) [43] [49] provides analytics services of which a KP Security Management-DE could request for such analytics services independently of whether the analytics services are offered by the MDAF or the NWDAF or complementarily by both functions. And having said that, both functions (MDAF/ NWDAF) may be needed by the KP DEs (the Security Management-DE and the other DEs of the KP Platform) at the same time depending on the analytics services that complement each other and yet implemented in the two functions separately. Given the type of analytics services required by KP DEs for certain autonomic operations objectives (use cases) targeted by KP DEs, the KP DEs can rely on analytics services provided by both MDAS (MDAF) and NWDAS (NWDAF). All what matters is that the two functions (MDAF /NWDAF) needs to be integrated with KP Platform such that the KP can selectively trigger or consume analytics services offered by the two functions according to the KP's DEs algorithms' targeted objectives. Such analytics services of the functions include User Equipment (UE) communications related analytics, UE mobility related analytics, abnormal behaviors related analytics, QoS related analytics, Service experience related analytics, NF load related analytics, network congestion related analytics, network performance analytics, and Slice load related analytics, etc.

Security Management-DE could request analytics services offered by the MDAS (MDAF) or NWDAF by describing the analytics that the MDAF or NWDAF should offer to the KP Security Management-DE. For example, upon a Security Management-DE having identified(detected) a general security threat, the Security-Management-DE may want to request for specific analytics

services per UE (User-Equipment) to be performed by the MDAS or NWDAF to identify the UE that is posing security problems. The Security Management-DE may want to request for analytics services only for a particular device (i.e. UE)) that has been subscribed to advanced security services. In addition, DE should dynamically request (on-demand) for the analytics services to be performed by the MDAF and/or NWDAF only when the services are needed in order to avoid loading the network with unnecessary traffic monitoring. The Monitoring-DE in association with the Security Management-DE should identify(deduce) the situation or context as to when the analytics services of the MDAS and/or NWDAF should be requested for and for which period of time are the analytics services required by the DEs (either continuously, periodically, or starting at a specific time and for a certain duration, etc.)

A Security Management-DE that subscribed to receive results of such analytics services of an MDAS or NWDAF could be triggered to take certain actions by events from the MDAS or NWDAF in case a certain device (UE) is showing some abnormal behavior (in terms of communications or mobility behavior).

The Security Management-DE might also be able to identify the traffic pattern, location pattern which need to be applied by the NWDAF or MDAF such that the NWDAF or MDAF does not need to learn the behavior of a certain device. An attack could be identified(detected) within other networks and could be used by the KP Security Management-DE and Monitoring-DE to define how to monitor abnormal behavior in their own network segment they are responsible for.

3.4. The Concept of Real-Time Security Threats Repository that can be implemented as part of the ONIX System of Federated Information Servers

The following diagram (Figure 9) illustrates the need for a Database or Repository (Real-Time Inventory) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies. Such a Database/Repository can be implemented as a member of ONIX System of Federated Information Servers. [19] presents ideas on how some ONAP Components can be used to implement a GANA ONIX Server and possibly ONIX's Multiple Federated Information Servers as well. According to the principles of federation of information servers of ONIX for the purpose of building up federated knowledge across the information servers, algorithms should be implemented on each of the ONIX member servers for the purpose of building links and associations among information elements stored on one information server with other information elements stored on other information servers. This then makes the federated ONIX servers appear as forming a single Information/Knowledge Base with correlated information elements, according to the extent to which relationships among information elements can be built. For example, the Information stored in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" can be linked by the construction of association relationships with information such as Services or Network Slices data stored on other ONIX servers. Such constructed relationships among information elements enable that the information in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" be enriched with other information such as Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies.

NOTE: The indicated Items may be stored in different Databases/Repositories instead, but it may be desirable to store them in the same Repository such that algorithms can be implemented on the Repository to keep the various items correlated to the extent possible and be kept updated in real-time.

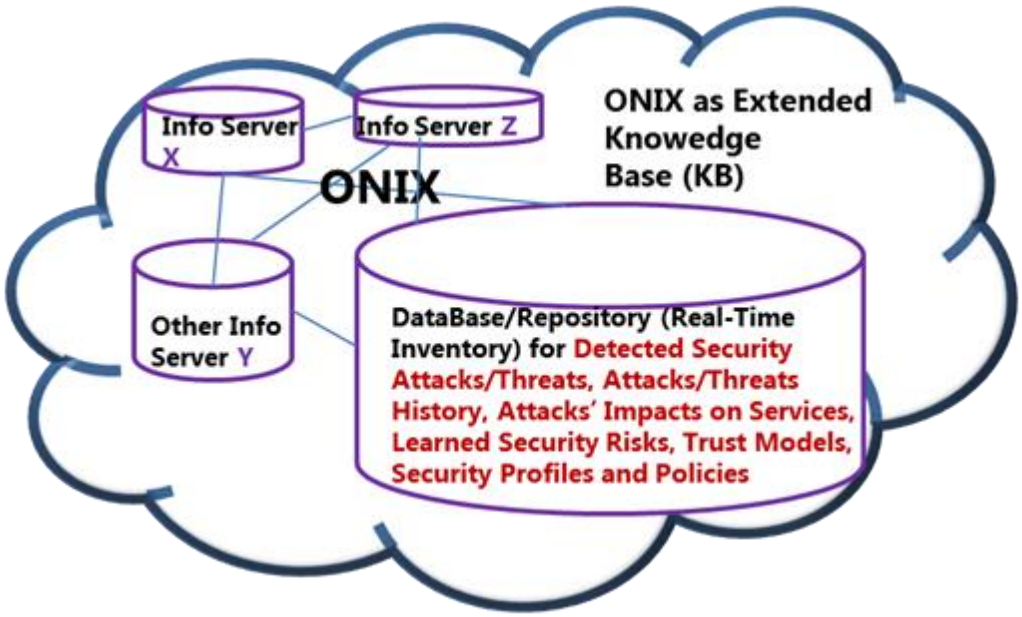

Figure 9: ***The Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies, as a Member of ONIX System of Federated Information Servers***

The following diagram (Figure 10) illustrates the concept of Federation of ONIX systems between two technical and/or administrative domains. A federation translation function (*Federation - "Model Based Translation Service" (F-MBTS)*) may be required if data models and communication methods for federations employed by the two domains are different.

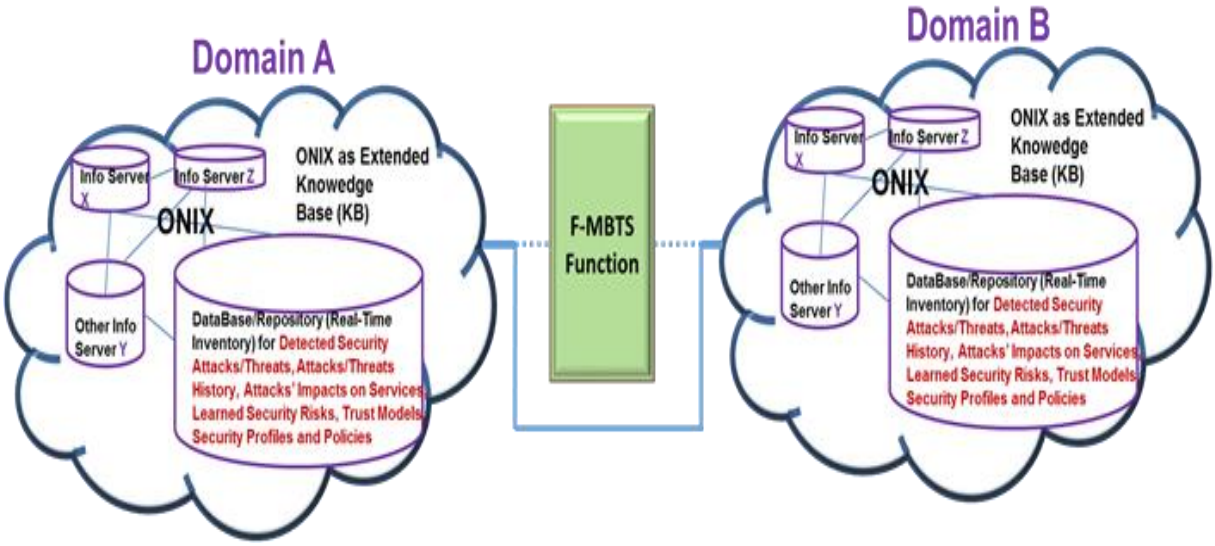

Figure 10: ***Towards Cross-Domain Federated ONIX Systems and Federated Databases/Repositories (Real-Time Inventories) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, and Learned Security Risks***

NOTE: In the cross-domains federations of *Databases/Repositories (Real-Time Inventories) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies*, some information may be constrained from being shared across two domains if the domains are administrative (e.g. two different network operators). For example, Trust Models, Security Profiles and Policies, may be constrained from leaking between domains.

ETSI TS 103 195-2[2] defines and describes the FMM Federation Reference Point that involves Knowledge Plane-to-Knowledge Plane communications, whereby MBTS services may be required between the KPs. [5], [6], [19], [22] and [25] discuss more details on Knowledge Plane to Knowledge Plane federations. Examples of Information that can be exchanged between Domains, e.g. between GANA Knowledge Planes across multiple Domains—information that may need to be exchanged between Peer Domains are illustrated below (including security related information), as extracted from the White Paper by NGMN [25]:

- **KPIs (examples):**
  - *Trust Levels (as measure of trustworthiness)*
  - *Threats Counts of potential impact "**To**" Peer Domain and Severity*
  - *Threats Counts of potential impact "**From**" Peer Domain and Severity*
  - *Aggregate state of the Domain in terms of Workload or Load Levels*
  - *Weights that are indicative of willingness of the Domain to deliver certain services (e.g. transport services)*
  - *Many Other Types of KPIs that function as security indicators can be identified and defined (and exchanged between KPs)*
- ***Other Types of Information***
  - *Domain Type(s): DT(s)*
  - *Domain Identifier : DId*
  - *Synchronization of actions across multiple GANA Knowledge Planes (KPs)*
  - *Security event information, e.g. Detected Threats/Incidents that may impact Peer Domain*
  - *Trust Models Information*
  - *Security SLA Violations unresolved*
  - *Load Situations and other types of Situations (e.g. as described in ETSI TR 103 404 and ETSI TR 103 473)*
  - *Various Types of Information and State Information that enable Multi-Domain State Correlation and resources programming by the GANA KPs for the collaborating Domains (e.g. Access, X-Haul (Fronthaul, MidHaul and Backhaul), Edge/MEC (Multi-Access Edge Computing), Data Center (DC), IP Backbone, and Core Networks, etc.), as outlined in ETSI TR 103 404 and ETSI TR 103 473 for examples.*

3.5. The Aspects of the Generic Framework that pertain to E2E Autonomic Security Management & Control across Multiple Domains (Network Segments)

The following figures illustrate the key layers (abstraction levels) by which collaborative autonomic security management and control can be achieved through the ETSI GANA Model principles, namely: (1) the **NE/NF Level**; and (2) the **Network Level**, by *NE/NF-Level (Node-Level) Security-Management Decision Element (DE)* and the *Network-Level Security-Management Decision Element (DE)*, respectively.

There are two options that can be pursued regarding implementing Federated GANA Knowledge Planes for E2E Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services. Figure 11 presents the **Option-A** (Horizontal Federation), by which the GANA Knowledge Plane (KP) Platforms for the specific network segments federate horizontally with each other without the need for an overlay Umbrella Hierarchical GANA Knowledge Plane (KP) Platform. Figure 12 presents the **Option-B** (Hierarchical Federation), by which the GANA Knowledge Plane (KP) Platforms for the specific network segments federate vertically through an overlay Umbrella Hierarchical GANA Knowledge Plane (KP) Platform that receives information from the lower level KPs and coordinates the lower level KPs.

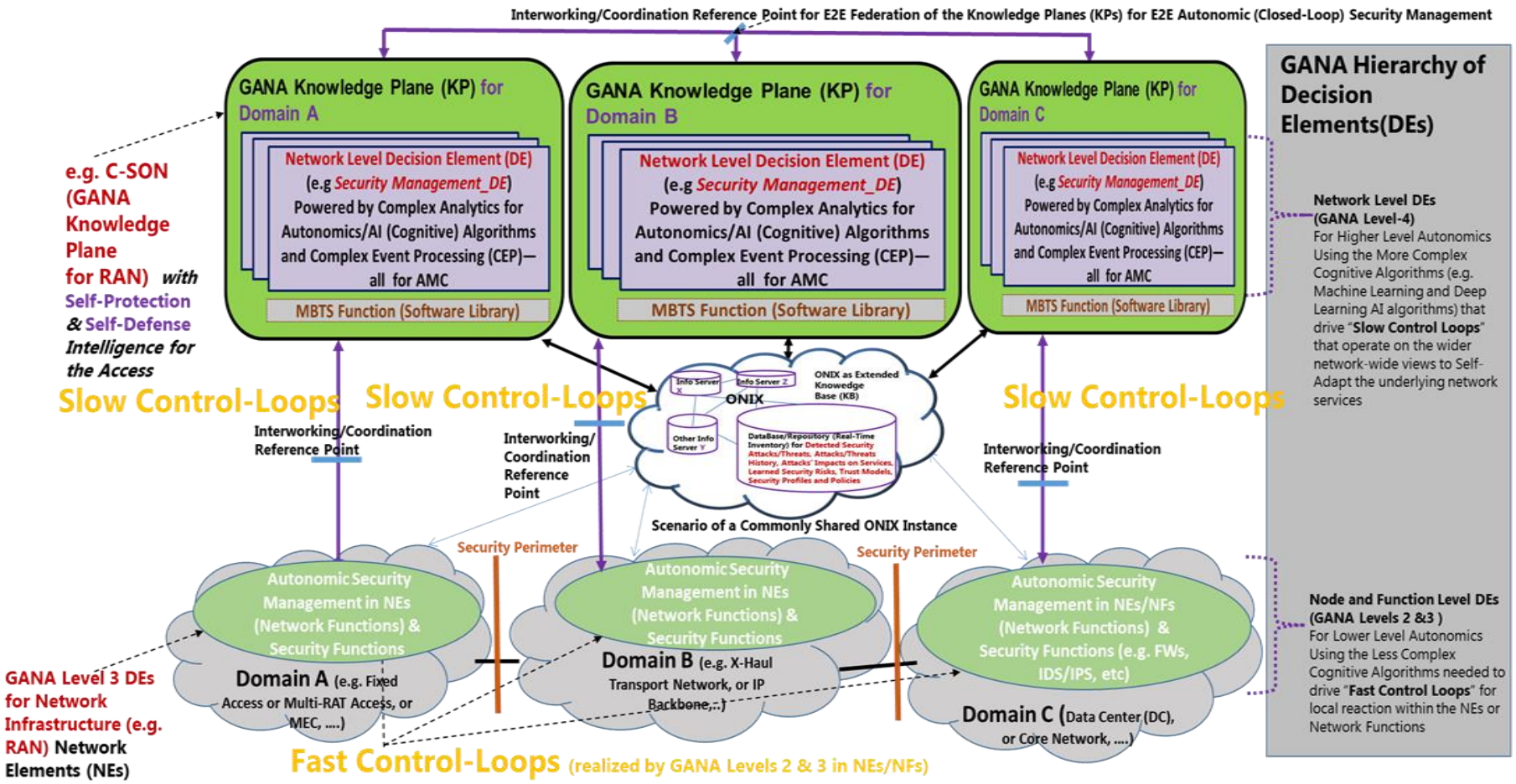

Figure 11: Option-A (Horizontal Federation), by which the GANA Knowledge Plane (KP) Platforms for the specific network segments federate horizontally with each other without the need for an overlay umbrella Hierarchical GANA Knowledge Plane (KP) Platform

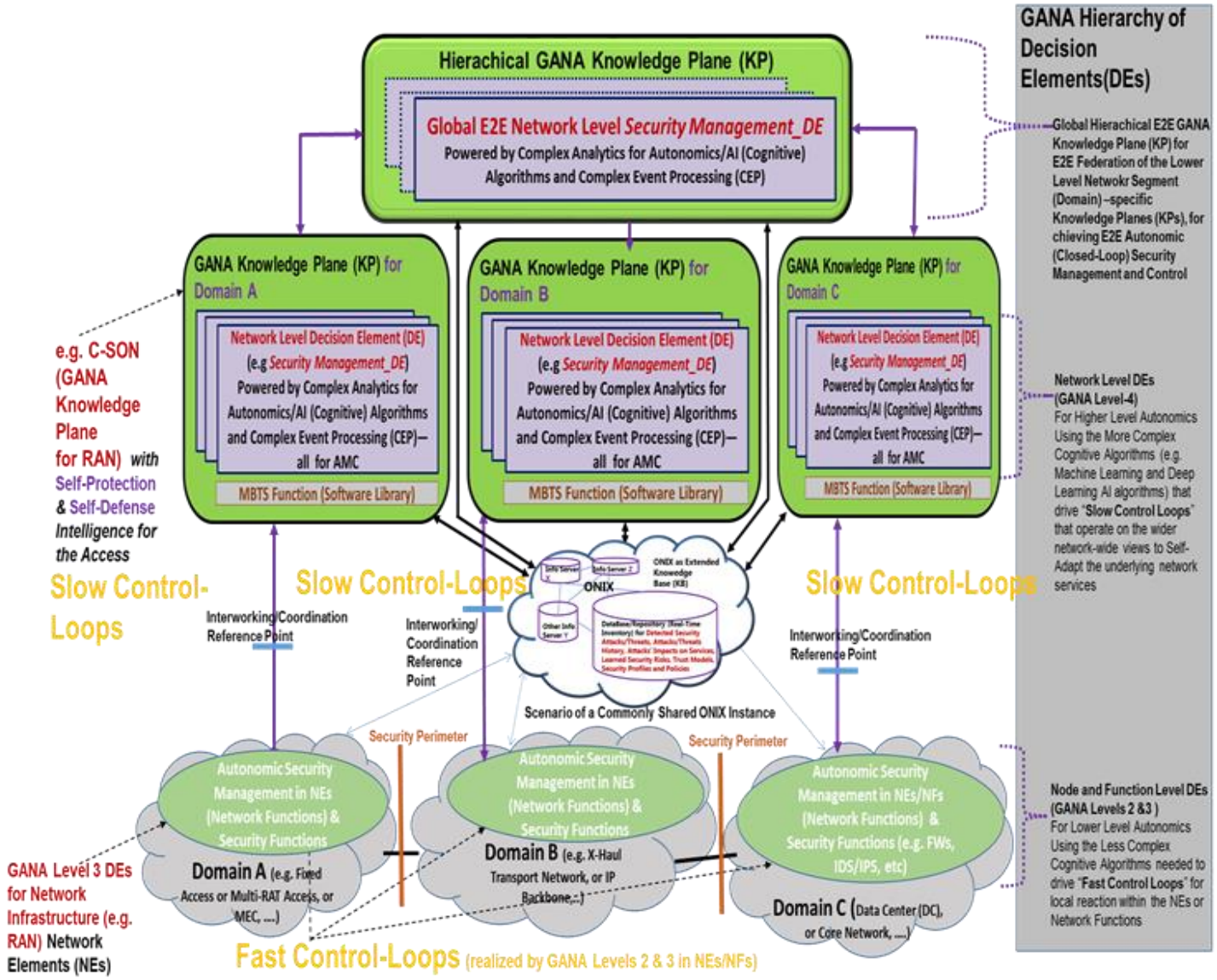

Figure 12: ***Option-B (Hierarchical Federation), by which the GANA Knowledge Plane (KP) Platforms for the specific network segments federate vertically through an overlay umbrella Hierarchical GANA Knowledge Plane (KP) Platform that receives information from the lower level KPs and coordinates the lower level KPs***

3.6. Check Point Capabilities for Implementing Federated Real-Time Security Threats Repositories as ONIX Repositories Federated across Multiple Network Operators

As the networking industry progresses to Autonomic and Autonomous Networks of the Future, there is a need to move to Model-Driven Information Networking for Networks, including Models for Knowledge Representation by way of federating diverse kinds of information servers and data collectors that may be deployed in a network operator's environment. There are various benefits of information federation such as dynamic and evolutionary building of correlated and linked information web that can be considered as the extended Knowledge Base (KB) for use in all autonomic management and operations of networks and services and the KB must be kept up-to-date in real-time. There is a need for data analytics algorithms and knowledge

synthesis algorithms that build knowledge using various information stored on information servers and data collectors and enable to build a network-wide real-time Knowledge Base. This can be achieved by the inter-working together of such algorithms running on the various information servers and data collectors to build links and associations of information and data across the various servers and collectors in the operator's environments. This is one of the purposes of the ONIX concept. Figure 13 illustrates the concept of Federation of Real-Time Security Info/Knowledge Repositories across Network Operators (as Multi-Domains). Considering Figure 13, the F-MBTS may be required if the format of information being federated and/or the protocols for the exchange of the information between the two participating domains differs and requires a mediation service of an F-MBTS function. Figure 13 presents a Check Point Capability for Implementing of Real-Time Repository for Threats Information using the Check Point ThreatCloud in each collaborating Network Operator Domain. Check Point ThreatCloud provides a capability concerning implementation of Real-time Inventories for Security Info/Knowledge & Federation of the Info across Multiple Network Operators. How to Use Check Point ThreatCloud Capability for Implementing the Real-time Inventory for Security Info/Knowledge and How Federation of the Info/Knowledge can be achieved across Multiple Operators and Multi-Domains.

NOTE: As discussed earlier in section 3.4, according to the principles of federation of information servers of ONIX for building up federated knowledge across the information servers, algorithms should be implemented on each of the ONIX member servers. This is for the purpose of building links and associations among information elements stored on one information server with other information elements stored on other information servers. This then makes the federated ONIX servers appear as forming a single Information/Knowledge Base (KB) with correlated information elements, according to the extent to which relationships among information elements can be built. For example, the Information stored in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" can be linked by the construction of association relationships with information such as Services or Network Slices data stored on other ONIX servers. Such constructed relationships among information elements enable that the information in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" be enriched with other information such as Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies. Therefore, apart from sharing (federating) information about detected or predicted security attacks and threats/risks among collaborating network operators, information about services or network slices and SLAs that may be impacted by detected security attacks or predicted risks may be federated as well, and also trust models. Such federations of information enable the receiver Knowledge Plane (KP) Platforms to compute and implement strategies aimed at defending their networks or creating back up services or resources to switchover customer services to in the face of security challenges. Such information federations may also serve as a basis for a KP to even compute and implement strategies aimed at dynamically selecting new peering networking partners that are more trusted in secure service delivery or security assurance in general.

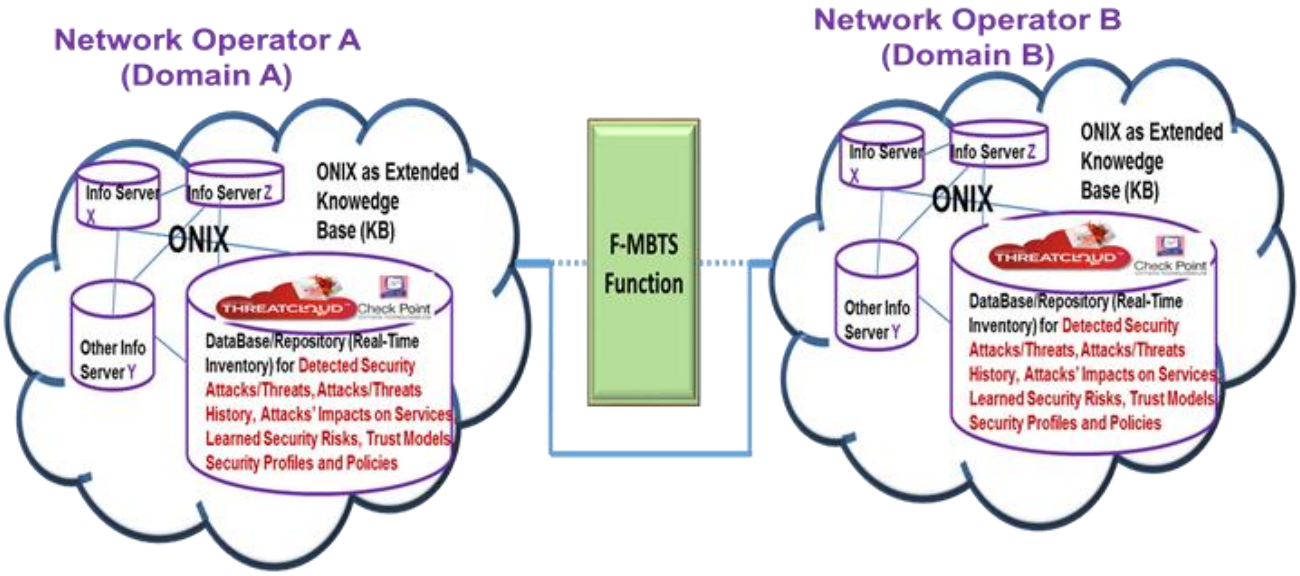

Figure 13: ***Implementation of Real-Time Repository for Threats Information using the Check Point ThreatCloud in each collaborating Network Operator Domain***

3.7. Why Security Analytics by the KP's Security Management DE may dynamically trigger and program On-Demand Monitoring of certain Traffic in the Network; and the role of Passive Probing & Analytics of Traffic copied from the Network

The figure below (Figure 14) presents a framework on Knowledge Plane (KP) driven "Open-Loop" and "Closed-Loop" (Autonomic) Service and Security Assurance for SDN Environments, with the desirable capability of the Security Management DE and the Monitoring DE of the KP in being able to collaboratively trigger On-Demand Traffic Monitoring in the Network. The figure shows some components that may need to integrate with a GANA Knowledge Plane (KP) Umbrella Analytics Platform for E2E Autonomic (Closed-Loop) Service and Security Assurance (powered by AI), and also an illustration on a Closed-Loop structure and the associated kinds of interactions between the KP Platform and SDN Controller(s) of the production network. To summarize the interactions flow between the entities in the depicted framework:

- By interacting with the SDN Controller of the Production Network, the Closed-Loop Analytics KP Platform Executes Remediation Strategies automatically by making Certain Configuration Changes to the Network via SDN Controllers for the Production Network. And the Analytics Platform (the KP) continuously *retrieves Health Scores data, Monitoring/Telemetry Data, Topology and Configuration-Data* from the SDN Controllers for the Production Network and from Network Elements/Functions (NEs/NFs) as well.
- Through the SDN Controller for the TAP & SPAN Aggregation Network, the KP DEs (particularly the Monitoring-DE) can trigger the SDN Controller to configure SPAN Sessions on-demand via SDN Controller for the Production Network to force copied traffic to flow to the Out-Of-Band (OBB) Visibility Aggregation Network that is programmable by the SDN controller for the OOB. The OOB is then programmed to forward traffic to various Analytics Tools in the Centralized Analytics Tools Farm (e.g. Probes and Security Analytics Tools). ETSI TS 103 195-2, [17] and [31] provide insights on how the Monitoring-DE (Network Level Monitoring DE) in the Knowledge Plane Platform can be implemented.
- There are other systems that can serve as Data Sources of the KP Platform, e.g. PM (Performance Management System) and FM (Fault-Management System) for Network and for IT (Information Technology) environments; and NEs/NFs
- The KP Platform may need to send some messages to the components and systems such as the ones indicated on Figure 14. For example, the KP DEs such as the Security Management-DE need to integrate with Ticketing Systems in order to consume events from the Ticketing Systems. The Security Management-DE may be interested in events that may be linked to security attacks incidents and use such events to compute and apply self-defense strategies for the network (the concept of self-defense is covered in more details in chapter 6). When a problem linked to a particular security incident related Ticket has been resolved and fixed by the KP as a whole, the Ticket is then cleared by the *KP Auto-Configuration_&_Auto-Discovery-DE* or directly by the *KP Security Management-DE*. The clearance of the Ticket is performed by the KP as "*Dynamic Updates*" on Tickets Resolutions/Clearance by KP DEs. i.e. the KP DE accesses the Ticketing System to clear the Ticket if the problem has been found and fixed by the KP.
- A human Service & Network Troubleshooter needs to primarily interface with KP Platform for certain needs linked to Service and Network Troubleshooting in case the KP is operating in an *"Open-Loop" Mode* in particular and the human in the loop is required during troubleshooting scenarios. The human user may choose to interact with the components marked as "Secondary Service Troubleshooting Position" when necessary.

The capabilities of the Security Management DE and the Monitoring-DE of the KP to trigger On-Demand Traffic Monitoring in the Network can be achieved by the Security Management-DE triggering (on-demand) the copying of traffic from the production network to Analytics Tools (e.g. Probes and Security Analytics Tools) by interacting with the SDN Controller of the Out-Of-Band (OBB). The SDN Controller of the OOB in turn interacts with the SDN Controller of the production network to create dynamic SPAN sessions on certain NEs/NFs to copy traffic to the OOB network. The Security Management-DE may instead go through the Monitoring-DE to cause it to trigger the process via the SDN Controller of the OOB Network and/or installing traffic-monitoring behaviors in certain NEs/NFs directly or via the SDN Controller(s) of the Production Network in addition. This is because the Security Management-DE continuously does analytics and correlation of various events to detect or predict security attacks or risks and may require to trigger, on-demand, the copying/probing and monitoring of certain traffic from the production network for analytics and for a certain duration. Moreover, this on-demand traffic monitoring may be triggered in addition to any traffic being currently monitored in the network and delivering meta-data or events data of interest to the Security-Management-DE. The Security Management-DE should communicate with the Monitoring-DE of the KP

so that the Monitoring-DE triggers the monitoring behaviors required by the Security Management-DE. ETSI TS 103 195-2, [17] [31] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE.

NOTE: [17] in particular, together with Demo material presented at the 5G PoC site in [17], present design principles for ***autonomic monitoring using the Monitoring-DE***. Figure 14 also illustrates this aspect by which Security Tools are dynamically fed with traffic that the Security Management-DE of the KP dynamically wants to be copied from the production network for a certain duration, monitored and analyzed by the Security Analytics Tools. The intelligence of the Security Management-DE may suspect that certain suspicious traffic is flowing in the network, and so it may decide to trigger the coping of suspected traffic from the network to Security Analytics Tools and obtain the results for further decisions. Such decisions may involve installing firewall rules to block the traffic or using the SDN controller of the production network for that. The OOB Aggregation Network and/or the SDN Controller of the Out-Of-Band (OOB) Network may supply to the Security-Management-DE (or the whole KP Platform) certain meta-data. The meta-data may include data such as KPIs & Metadata created out of raw traffic copied from the production network by the Visibility Solution in place for a particular network (e.g. IETF standardized IP Flow measurements metadata such as *sFlow, NetFlow/IPFIX, etc.*).

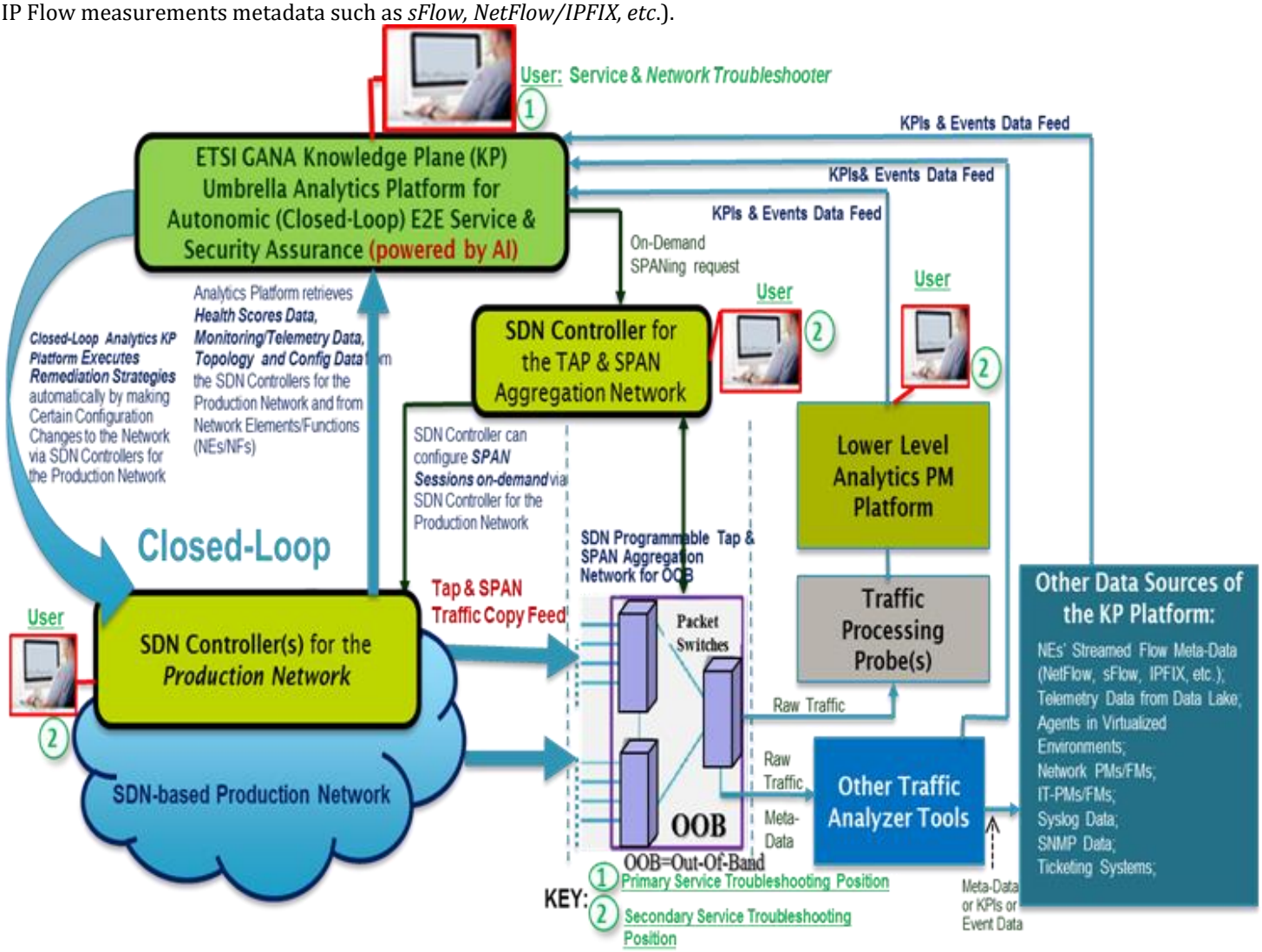

Figure 14: ***Knowledge Plane (KP) driven "Open-Loop" and "Closed-Loop"(Autonomic) Service and Security Assurance for SDN Environments, with the capability of the Security Management-DE and the Monitoring-DE of the KP in being able to collaborate in triggering On-Demand Traffic Monitoring in the Network for Analytics of Suspected Traffic***

4. Security Functions Placement/Orchestration in 5G and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics; Security-DEs Orchestrations

Types of Placement and Orchestration of Security Functions and Security Management-DEs specific to a Network Slice:

1. Static Placement/Orchestration of a Security Function: Security Functions that come in form of Physical Network Functions(PNFs) and those hosted in NEs/NFs in form of PNFs such as some routers or switches are statically placed at specific points in the network topology and infrastructure. Orchestration aspects at such functions involves security service orchestration by simply configuring the physical security function to perform the security enforcement role.

   NOTE: Programmability requirements aspects for security functions are covered in the next section.
2. Dynamic Placement and Orchestration of a Security Function: There are security functions that can be dynamically instantiated as Virtual Network Functions (VNFs), and such VNF based security functions can be dynamically instantiated (placed) at any desirable point in the network where a Network Functions Virtualization Infrastructure (NFVI) environment is available for orchestrating and managing the VNFs' lifecycles. Orchestration aspects at such functions involves instantiations using a MANO stack and performing the configuration of the virtualized security function.

   NOTE: Programmability requirements aspects for security functions are covered in the next section.

3. Security Management-DEs Orchestration: Every network segment should have a GANA Knowledge Plane (KP) Platform associated with the network segment as illustrated in this White Paper. A single instance of a KP Platform is assumed to be responsible of the whole network segment and slices instantiated in that network segment. However, there may be some need to scale the KP Platform or its components according to the size of the network and workload, bearing in mind that the KP Platform may be deployed as a Virtualized Platform. Orchestration and Configuration of the KP Platform's components such as DEs can follow the approach presented in ETSI TS 103 195-2. Here, we assume that for network slices instantiated in the network segment the expectation is that a single KP Platform and its Security-Management-DE instance is responsible for service and security assurance of all the Slices instantiated in the underlying network segment. In the underlying NEs/NFs of the network, particularly in those in which a security function or service is required, a single Node-Level Security-Management-DE associated with the NE/NF needs to be orchestrated and configured to realize the "*fast control-loop" for self-protection and self-defense* from the viewpoint of local observations on whether security is being compromised. The NE/NF level Security-Management-DE is also expected to listen for any policy changes from the KP level Security-Management-DE and apply them while also participating in synchronizations of actions for guaranteeing *stability of control-loops* as prescribed in ETSI TS 103 195-2. The NE/NF local DEs are called "dDEs" (distributed DEs). "dDEs" are the DEs implemented to operate in Network Elements/Functions (NEs/NFs) to realize the "*fast control-loops*" and also to implement distributed control-loops within the network infrastructure through horizontal interactions with other dDEs across a network scope. Such dDE horizontal interactions relate to a form of "in-network management"—in the case when implementer(s) of the autonomics chose to implement the autonomics through a distributed algorithm than using a centralized approach through the KP level DE(s).

NOTE: In this White Paper the subject of security functions placement is also discussed in other chapters of this White Paper (particularly chapter 7).

Regarding autonomic/dynamic orchestration of security enforcement policies as driven by Network Slicing Dynamics and Security Management-DEs orchestrations, the following aspects come into play:

- The framework for service and security of assurance of network slices is required to be integrated with the framework for Slice Service Fulfillment (including Slice Creation and Orchestration). When a Network Slice definition has been created and passed to platforms used for the provisioning of the slice some data about the Slice Definition data should be passed to the Knowledge Plane (KP) Platform responsible for the service and security assurance of the slice. This means a "*Specification*" of the Network Slice's Objects and Parameters for configuration and the associated

Configuration-Data should be passed to the KP Platform as necessary. The KP Platform's Security Management-DE, Monitoring-DE, and QoS Management-DE in particular, need to be provided with the specification of the inputs data pertaining to Slice Definition data (including associated SLAs definitions). They need such inputs in order to perform autonomic service and security assurance of the slice, while also participating in federation with other peer DEs in other KP Platforms within the single Network Operator (as Domain) and across partnering (peering) Network Operator Domains.

NOTE: The subject of the various kinds of data/information that can be supplied as ***inputs*** for the operation of a Knowledge Plane (KP) is covered in ETSI TS 103 195-2.

- Orchestration and Configuration of the Security Management- DEs of the various Knowledge Plane Platforms to be involved in E2E Autonomic (Closed-Loop) Service and Security Assurance of the E2E Slices.
- Collaborations that may be required between a Security-Management-DE and a DE in the same KP Platform, e.g. a QoS Management-DE and a Monitoring-DE, which programs the required monitoring services in the network. The key design question that needs to be addressed here, with respect to the collaborations of the DEs, is to identify system-critical and other resources in the network and information base that are relevant to the two non-functional feature categories that need to be enabled in connection with slicing, namely: security and resource management (including QoS). If Resource X and Resource Y are both relevant to an End-to-End or Single-Tier Slice A, then the orchestration and/or (re)-configuration of a Security Functions (SFs) and QoS Functions (QFs) required by the Slice should be jointly (collaboratively) put into consideration by the Security-Management-DE(s) and QoS-Management-DE(s), respectively, in order to see how to access, modify, block, or release Resources X and Y so as not to affect the integrity of Slice A or the proper functioning and consistency of state and information from either SF perspective, QF perspective, or a global overall perspective. Following GANA principles (in ETSI TS 103 195-2 and [17] [31]), the Security Management-DE should communicate with the Monitoring-DE of the KP so that the Monitoring-DE triggers the monitoring behaviors required by the Security Management-DE. ETSI TS 103 195-2, [17] [31] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE. The Security-Management-DE then consumes the monitoring data it requires from the network as necessary for its autonomic behaviors. The Security-Management-DE may require to coordinate with other DEs of the KP Platform, e.g. the QoS Management-DE, to coordinate on joint actions in reaction to impact of detected or predicted attacks on a network slice. The same applies for the QoS Management-DE, it should communicate with the Monitoring-DE of the KP so that the Monitoring-DE triggers the monitoring behaviors required by the QoS Management-DE. The QoS Management-DE then consumes the monitoring data it requires from the network as necessary for its autonomic behaviors. Such that when QoS requirements and SLAs for the Slice are being challenged (as per monitored network conditions and incidents), the QoS Management-DE can (re)-tune QoS provisioning mechanisms of the network adaptively. In addition, or alternatively, the QoS-Management-DE may communicate with the Security-Management-DE so that the DEs can jointly compute paths or resources that can be created or switched over to by traffic flows such that QoS SLAs and Security SLAs for the Slice are jointly assured. Such DEs coordination may require the participation of the Monitoring-DE and/or other DEs of the KP Platform.
- Behaviors expected of Security Management DEs of each KP Platform in response to various dynamics of network slices and security problems that may be detected or predicted concerning their impacts on specific slices and SLAs. Some scenario examples that convey this conceptual idea are as follows:
    - In an End-to-End slice covering the tiers of access, edge, metro, transport, and core, the Security-Management-DEs of the KP Platform of each tier may use different security mechanisms in each tier for anomaly or threat detection regarding which parameters and patterns are analyzed (differently for each tier) to detect and mitigate potential threats or attacks on the network that are affecting the slice under protection and many other valuable/critical resources
    - When specific SLAs are binding, even on an E2E slice, the implementation and the mechanisms for achieving this same SLA often differ and depend on what tier is under question. For instance, protecting with encryption or fingerprinting/signature an application flow/stream which is part of a slice is different in terms of the mechanism used on the edge and access part of a network as compared to that in the transport or even core part. As illustrated on Figure 15, the Framework recommends to have a set of Knowledge Planes (KP), each of which covers one tier of the E2E chain, and having a distinct type of security mechanism for the same functionality. Upon federating those KPs to cover the E2E path, the various security mechanisms for the same functionality would be aligned and streamlined to form an E2E consistent service.

- Examples of data and messages that may be exchanged by the KP Platforms involved in the E2E Federation to effect actions by other KP receiving the data and messages include but are not limited to:
    - State messages regarding behavioral information detected or deduced based on the captured and processed metrics in a KP covering a specific tier of the E2E chain; this information helps other KPs which cover other tiers of the E2E chain in their decision-making process and actions and enable consistency and synergies in the operation of the functions under focus (security functions, resource management (incl. QoS) functions) on an end-to-end basis across multiple KP Platforms
    - Specific state messages regarding the status of e.g. encryption or anomaly detection in a specific KP (and its corresponding tier) passed on to an adjacent federated KP platform
    - Other kinds of data and messages as described in the section 3.4 and in NGMN's 5G E2E Architecture Framework [25] and [18].

The following figure (Figure 15) illustrate the aspect of Federation of Security Policy Enforcement Engines (namely Security Management DEs) over the value chain tiers (Access/Edge, Transport, Core, etc.) with End-to-End Slices.

NOTE: The lower part of the Figure 15 is based on the Figure 4 that is readable.

The other aspects discussed in this White Paper on E2E Federation of GANA Knowledge Plane (KP) Platforms complement the Figure 15.

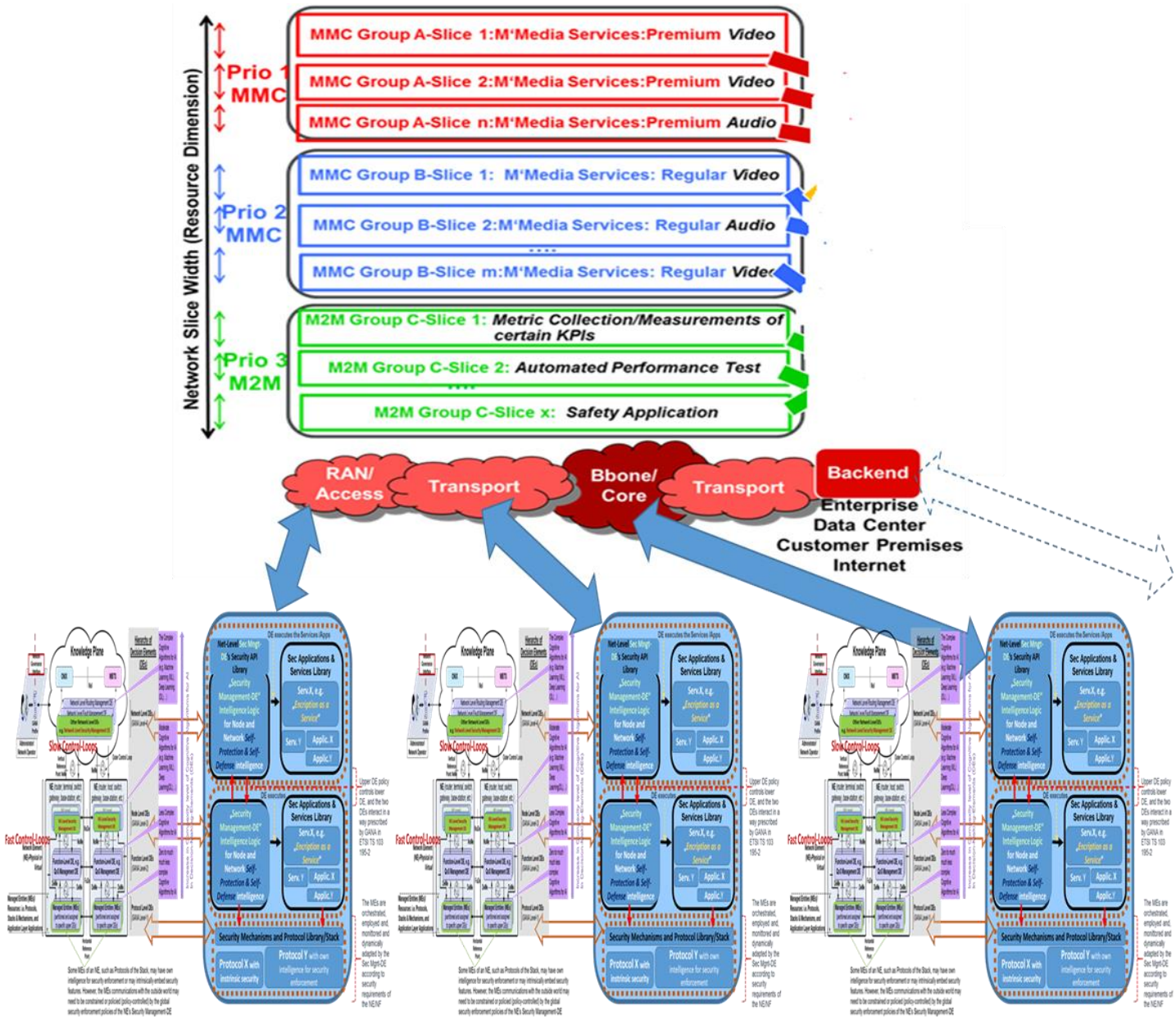

Figure 15: ***Federation of Security Policy Enforcement Engines (namely Security Management DEs) over the value chain tiers (Access/Edge, Transport, Core, etc.) with End-to-End Slices***

5. Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection and Threats/Risks Predictions

Security Functions such as Firewalls, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) need to expose programmatic interfaces through which Security-Management-DEs can program the functions by adaptively configuring them with security policies that must be applied by the Functions. While at the same time the security functions should enable the Security Management-DE to obtain/receive events data, KPIs data, and logs from the Functions (Network

Elements). Check Point is a supplier of Security Functions that are programmable and enable implementers of Security-Management-DEs to program them as driven by the intelligence of the DEs, as illustrated by Check Point security functions/platforms programmability presented in section 7.2.

Based on the structural model for realizing/implementing AMC Control-Loop(s) of a Security Management-DE meant to operate at Network Level (in the GANA Knowledge Plane (KP) Platform), the figure below (Figure 16) provides insights on an example of how a Security Management-DE that operates on network level (in the Knowledge Plane (KP) Platform) can be implemented. This refers to implementation guide terms of the various data and event sources that can be considered by the implementer/supplier of the DE, and the systems and components the DE may need to interact with for various purposes. For example, the DE may interact with the various entities indicated, for the purpose of programming security functions or causing resource or service backup entities to be orchestrated and instantiated. Below, we provide a summary of some of the entities that the Security Management-DE should be able to interact with (the numbers on communication flows are simply there to distinguish the types of interactions and not necessarily the ordering of the communications), and the reasons for the desired interactions:

- **Orchestrator**: The interaction between an Orchestrator (e.g. Service Orchestrator) with a GANA Knowledge Plane (KP) Platform in general relates to the KP's need to consume events that an Orchestrator may be able to propagate to the high level platform (i.e. the KP). KP consumption of such events is needed for its Complex Event Processing (CEP) and capabilities in reasoning about the state of the network and computing plans of actions as necessary. The events may be of interest to all the KP DEs or to specific DEs such as the Security Management-DE. The interaction is also for the purpose of the KP's needs to invoke the services of the Orchestrator dynamically based on the requirements for adapting the underlying network or to orchestrate new instances of resources or services in a strategy to remediate and ensure continuous network services delivery and guarantee SLAs and security. The KP DEs also need to consume various kinds of KPIs that may be shared by the Orchestrator. KP strategies such as remediation against problems may be applied reactively or proactively to detected or predicted problems, respectively. More details on this subject can be found in ETSI TS 103 195-2 and [5] [19] [17] [22] [26].
- **SDN Controller of the Production Network**: The interaction involves the KP Platform being able to (re)-configure (program) the network via the SDN controller. The interactions also involve the SDN Controller dynamically supplying Information to the KP Platform, e.g. Topology Data, Telemetry, Health scores data (concerning the underlying network), Configuration-Data (as configured for dissemination to the KP by the *KP level Monitoring-DE* on the SDN Controller). The configuration on the SDN Controller, regarding the data and information the SDN Controller should disseminate to the KP platform or Data Lakes may be done by the *KP level Auto-Configuration_&_Auto-Discovery-DE*. As discussed in [5] [19] [17] [22] [26], the KP Platform may selectively program the network directly via the SDN Controller or other management and control systems available in the environment
- **Monitoring-DE in the KP**: The interactions that may be implemented, regarding KP DEs such as the Security-Management-DE interacting with the Monitoring-DE are as follows: All the KP DEs may express monitoring needs, regarding the specific needs to receive monitoring data from the network, to the Monitoring-DE implemented as part of the KP Platform. The Monitoring-DE in turn configures and tunes the monitoring services of the network (including monitoring services/functions within the NEs/NFs and also the Out-Of-Band (OOB) traffic copying and analytics tools). For more details on the subject of the functionality of the KP level Monitoring-DE, readers should refer to ETSI TS 103 195-2. The other source that offers important insights on Autonomic Monitoring functionality and services of the Monitoring-DE at KP Level is [17]. ETSI TS 103 195-2, [17] [31] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE, including insights on how the Monitoring-DE (Network Level Monitoring DE) in the Knowledge Plane Platform can be implemented in general.

  NOTE: [17] in particular, together with Demo material presented at the 5G PoC site in [17], present design principles for ***autonomic monitoring using the Monitoring-DE***. Also, when it comes to monitoring in NFV environments, ETSI GS NFV-REL 004[55] and ETSI GS NFV-SEC 013[54] provides very useful insights on monitoring in virtualized environments, including Security Monitoring in such NFV environments.

- **SDN Controller of the Out-Of-Band (OOB) Visibility/Aggregation Network:** The Security Management-DE may require that some traffic be copied from the network on-demand, to the Out-Of-Band(OOB) Visibility Network. The traffic is then analysed by some Analytics Tools in the Tools Farm and results in form of KPIs or Detected Network Events be communicated by the Analytics Tools to the Security Management –DE in the KP Platform. The Security-

Management-DE may trigger this via the Monitoring-DE in the same KP Platform to which the Security Management-DE belongs (as shown on the figure), instead of directly interacting with the SDN Controller of the Out-Of-Band (OOB) Network. The intelligence of the Security Management-DE may suspect that certain suspicious traffic is flowing in the network, and so it may decide to trigger the coping of suspected traffic from the network to Security Analytics Tools and obtain the results for further decisions. Such decisions may include installing firewall rules to block the traffic or using the SDN controller of the production network for that. The OOB Aggregation Network and/or the SDN Controller of the Out-Of-Band (OOB) Network may supply to the Security-Management-DE (or the whole KP Platform) certain meta-data such as KPIs & Metadata (e.g. IETF standardized IP Flow measurements meta-data created from the raw traffic copied from the network such as *sFlow, NetFlow/IPFIX, etc.*). There are various ideas on how such Metadata can be used in security attack detection or predictions, e.g. the following sources provide insights on this subject: [32] [33] [34] [35] [36] [48].

- **Data Lake:** Various Data that may be available through a Data Lake may be of interest to the Security Management-DE to consume in form of the raw data or in form of knowledge that may be synthesized by Data Analytics/AI algorithms running on the Data Lake.
- **NEs/NFs (e.g. Router, Switch) and security-specialized NEs/NFs such as Security Functions such as IDS (Intrusion Detection System), FW (Firewall), IPS (Intrusion Prevention System), Network Data Analytics Function (NWDAF) defined by 3GPP** [43] [49]**, Management Data Analytics Service (MDAS) defined by 3GPP** [44]**.** The Security Management-DE may interact with the NEs/NFs directly in order to dynamically program them to install security policies, and also to receive KPIs, Event & Log data feed that may be required by the Security-Management-DE's Algorithms (and even by other KP DEs), from the NEs/NFs.
  NOTE: Sections 3.2 and 3.3 provide detailed insights on this subject.

- **MANO (Management and Orchestration) Stack**: The Security-Management-DE may decide to orchestrate via the MANO, the instantiation of some security functions in response to some security attacks or vulnerabilities/risks/threats detected or predicted. KPI & event data feed from the instantiated security functions need to flow to the Security Management-DE. With a that, "*Remediation Actions*" against detected or predicted security attacks/threats/vulnerabilities may be executed by the Security Management DEs on certain NEs/NFs such as the security functions instantiated as Virtual Network Functions (VNFs).
- **Ticketing Systems**: The Security Management-DE needs to integrate with Ticketing Systems in order to consume events from the ´Ticketing Systems that may be linked to security attacks incidents and use such events to compute and apply self-defence strategies for the network (the concept of self-defence is covered in more details in the next chapter (chapter 6)). When a problem linked to a particular security incident related Ticket has been resolved and fixed by the KP as a whole, the Ticket is then cleared by the Security Management-DE as Dynamic Updates on Tickets Resolutions/Clearance by KP DEs, i.e. the DE accesses the Ticketing System to clear the Ticket if the problem has been found and fixed by the KP.
- **ONIX**: The Security Management-DE needs to exercise Information Storage and retrieval from ONIX by the DE, particularly with the DataBase/Repository (Real-Time Inventory) of the ONIX that stores Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies.

NOTE: Check Point offers capabilities that enable to implement Security Management-DE and the Control-Loop(s) Structure presented in this section. Chapter 8 provides details on the subject of the enabler capabilities available in Check Point platform that can be leveraged in implementing a Security Management-DE, namely: **Firewall Security Functions**, the **Data Lake**, and an **ONIX Real-Time Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks**. Those Check Point capabilities are complemented by the much broader and core Check Point capabilities discussed in chapter 7.

Figure 16 presents a desirable capability of the Security Management DE to operate in Open-Loop and Closed-Loop Mode and its operation in Correlation and Autonomic Security Management & Control.

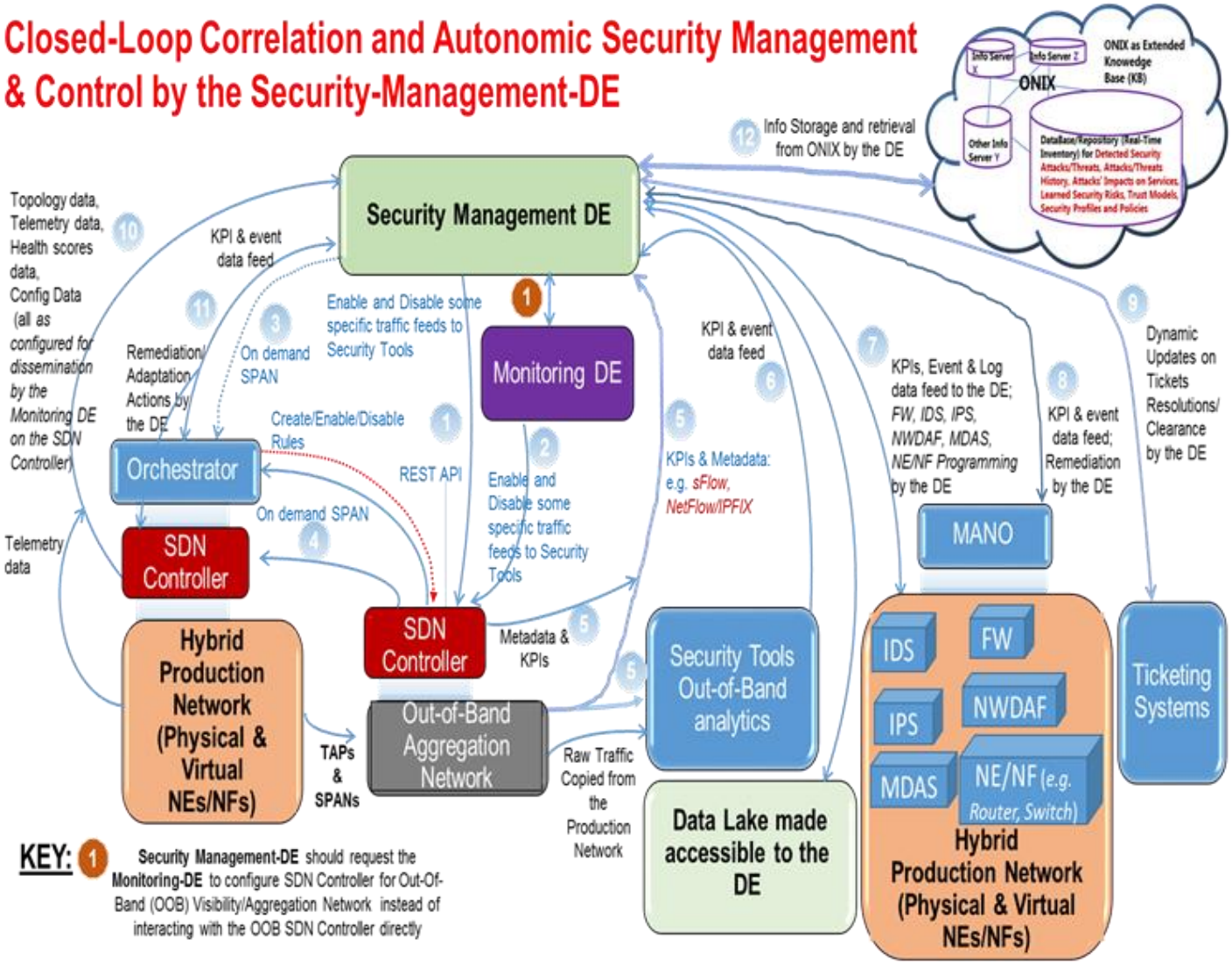

Figure 16: ***Capability of the Security Management DE to operate in Open-Loop and Closed-Loop Mode and its operation in Correlation and Autonomic Security Management & Control***

6. Implementing "*Self-Protection*" & "*Self-Defending Behaviors*" for specific Network Segments/Domains by GANA KP Platforms, within Single Network Operator and across Multiple Network Operators

This chapter provides insights to implementers of autonomic (closed-loop) security management and control on how to leverage research results emerging from various R&D projects on Autonomic/Cognitive Networks (i.e. Self-Organizing/Self-Adaptive Networks) and their associated Autonomic Management & Control Systems. Leveraging such results in implementing Security-Management-DEs that are based on the ETSI GANA standard and conform to the Framework presented in this White Paper. It is possible to map the features prototyped in the various R&D projects, with respect to security management components that employ AI in automating security policing and dynamic network and service security management aspects, to Security Management–DEs meant to operate at specific GANA Levels. That enables to implement the DEs that fully conform to the ETSI GANA standard and the Framework presented in this White Paper. With the definitions of *Self-Protection* and *Self-*

Defense provided earlier, implementers of Security-Management-DEs can be guided accordingly on how to make a DE exhibit both capabilities/features. And implementers can use the definitions in mapping the features prototyped in the various R&D projects, with respect to security management components that employ AI in automating security policing and dynamic network and service security management aspects, to Security Management–DEs meant to operate at specific GANA Levels. Then they can transform the prototyped components into products that conform to the GANA standard and the Framework, accordingly. For example, the following sources provide insights on some prototype implementations of components for implementing ***self-protection and self-defending strategies and behaviors for the network*** [21] [23] [24] [27] [28] [30]. Additionally, the following sources provide some insights that can help implementers of Security-Management-DEs' self-protection and self-defense behaviors for the network and its services: [37] [38] [39] [40] [41] [42] [45] [51]. [47] provides useful insights on automated security policies road-mapping. [20] provides useful insights for consideration in tools for network automation that can also be considered when implementing KP DEs in general.

The following are example Use Case Scenarios for **Self-Protection** and **Self-Defense Behaviors**:

- A Use Case on **Self-Protection** of the Network within Single Network Operator and across multiple Network Operators: User-plane integrity, roaming security, and flash-network traffic are use case scenarios where self-protection within 5G can be very essential. In a partially proactive manner, the security system can check the cryptographic protection integrity of the use data plane at regular intervals and report in a timely manner via a trigger if any anomaly is detected. This way, the protection of user plane data and its integrity from a security (and mainly cryptography) viewpoint is established. When it comes to roaming, updating security-parameters related to roaming in 5G as users move across multiple operators is a key aspect; for proper self-protection, those parameters need to be passed on in real-time, processed correctly, mapped among operators, and also protected from unauthorized access. Flash network traffic is a use case which comes into play upon a massive amount of entities and/or messages they generate, typically, e.g. in an IoT (or massive-IoT) scenario in 5G. For appropriate self-protection, differentiated scaling of the control and data planes by the collaboration of the GANA Knowledge Plane (KP) Platforms and management and control systems (including MANO stack) responsible for each network segment has to be done. CUPS (Control and User Plane Separation) is a significant step towards standalone 5G. The intelligence of the GANA KP Platform(s) to dynamically orchestrate and/or scale control and data plane functions include KP(s) strategies to address autonomic slice service fulfillment, service assurance and security assurance requirements (SLAs), and such KP operations include both, single KP and KP federated operations. The self-protection strategies by the KP Platforms shall put in place (trigger) the monitoring of each of the planes and adjust the scaling accordingly in order not to overload any of the planes with massive requests.
- A Use Case on **Self-Defense** of the Network within Single Network Operator and across multiple Network Operators. A signaling storm and a DoS attack on the infrastructure (as opposed to a DoS attack on the end-user device level/tier) are two out of many other scenario examples that confront 5G systems with significant threats and where systematic self-defense mechanisms and strategies that a KP Platform should orchestrate are essential in mitigating those threats. With many distributed control systems being directly or per-proxy coordinated and managed by 5G, mechanisms analogous to NAS (Non Access Stratum) in 3GPP such as EPS Mobility Management (EMM) and EPS Session Management (ESM) use signaling to set the scene for 5G-based data transfer and application flow. A popular attack type and eminent threat is producing a signaling storm, meaning an "strongly inflated beyond manageable bounds" amount of messages (e.g. NAS EMM and ESM), causing the draining of system-critical bottleneck resources in the processing (signaling, control chain). Self-defense in 5G by KP Platforms within a single operator or across multiple operators would activate a protective shield for critical resources and entities, e.g. the ones preforming NAS functionality including EMM and ESM, and then throttle the flow of incoming signaling requests that collectively form the attack.

7. Key Check Point (Network Security Solutions Vendor) Capabilities that help implement the GANA based Generic Framework for E2E Autonomic Security Management and Control

7.1. Check Point Capabilities for Implementing the ONIX System's Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks, together with Illustration of a "*Security Management-DE Implementation*"

NOTE: This whole chapter 7 and its sub-sections present how the Capabilities of Check Point Solutions can be used to implement the outlined Generic Framework for E2E Autonomic (Closed-Loop) Security Management and Control, in terms of the extent to which Check Point Solutions can be used to implement the Framework. Chapters 8 and 9 provide additional complementary details on how to use Check Point Capabilities to implement GANA KP Security Management-DEs.

This section illustrates the Check Point Capabilities already available for *Implementing Security Management-DE and Real-Time Repository for Threats Information using the* ***Check Point ThreatCloud***. Figure 17 presents an implementation of Security Management-DE and Real-Time Repository for Threats Information using the Check Point ThreatCloud.

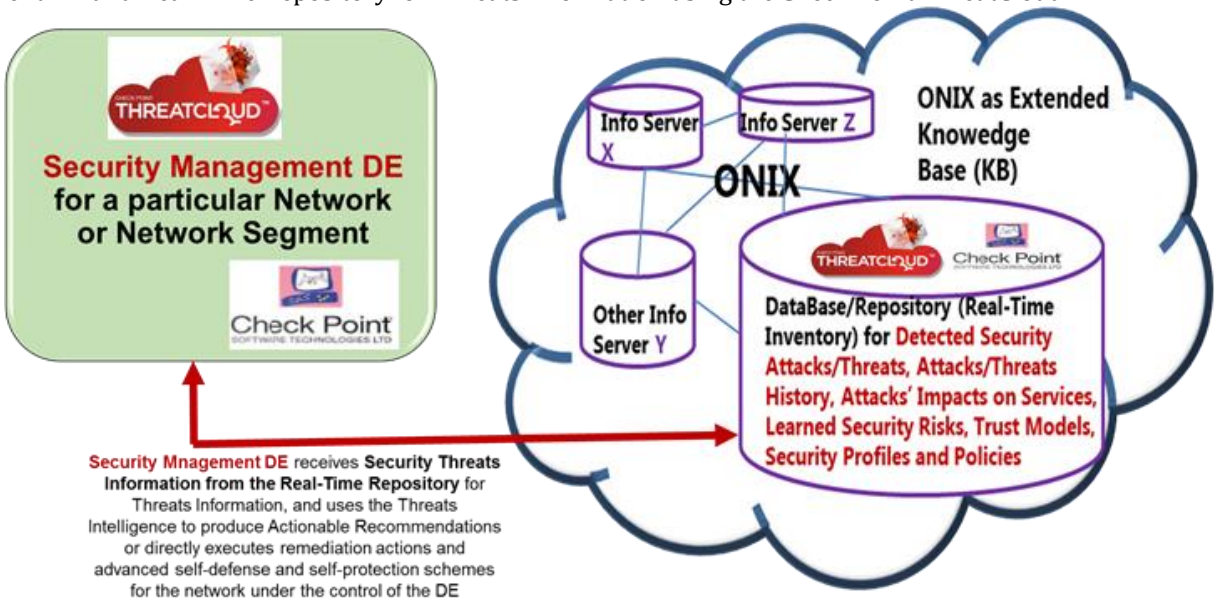

Figure 17: ***Implementation of Security Management-DE and Real-Time Repository for Threats Information using the Check Point ThreatCloud***

7.2. Overview on Check Point Capabilities on Security Functions for Telco-Clouds and 5G Network, Programmability, and How to integrate with GANA Knowledge Planes (KPs)

The figure below (Figure 18) presents the capability of the Virtualized Check Point Security Management Component (as an EM), to expose events and some data to the Security Management-DE in the Knowledge Plane Platform, and also expose an API through which the Security Management-DE can dynamically program it and ultimately the Check Point Security Gateway (as a VNF). ETSI GS NFV-SEC 013[54] provides useful insights on security problems that can be detected or predicted in an NFV environment that can be addressed by DE KP algorithms and autonomic operations.

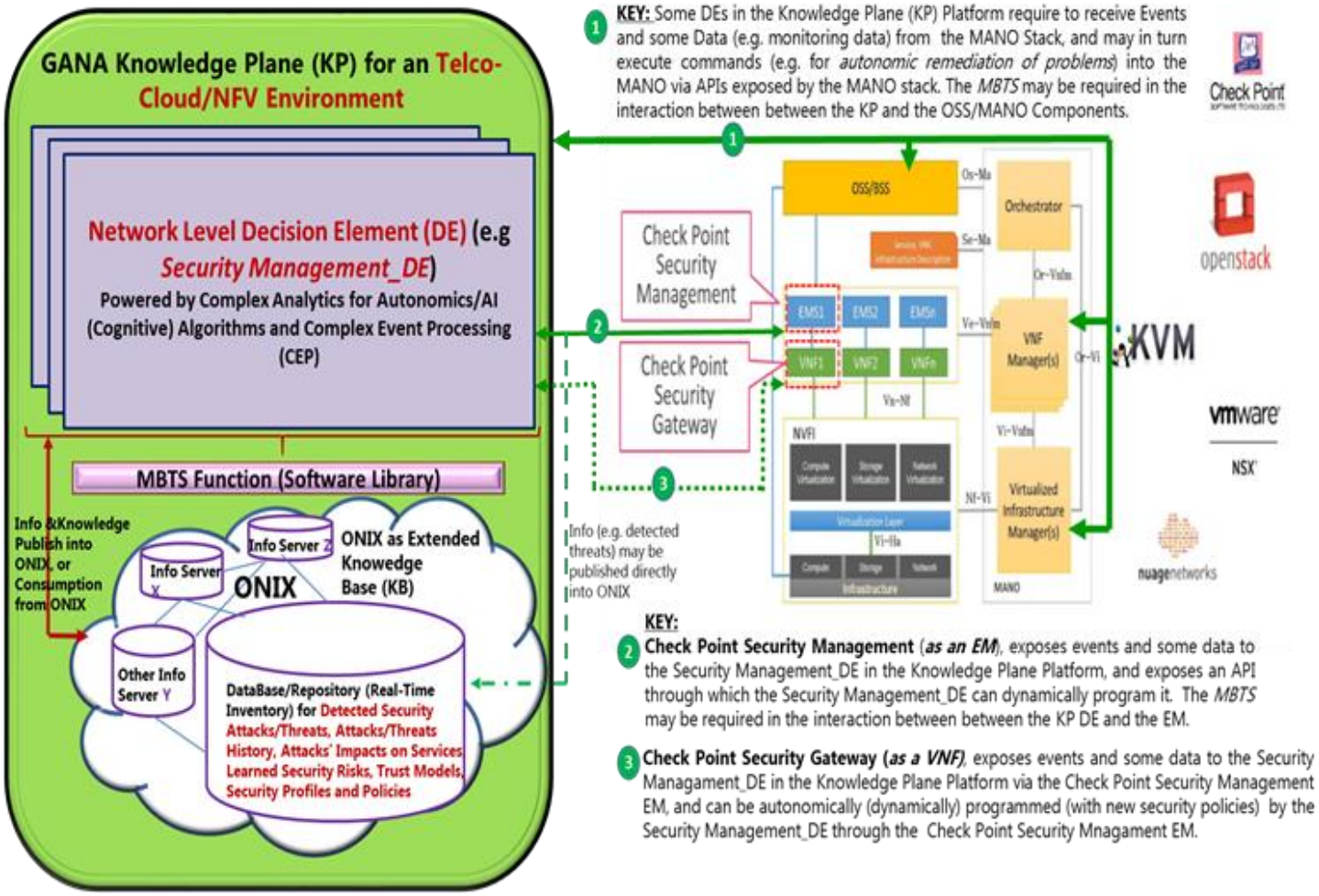

Figure 18: ***The Capability of the Virtualized Check Point Security Management Component (as an EM), to expose events and some data to the Security Management_DE in the Knowledge Plane Platform, and expose an API through which the Security Management_DE can dynamically program it and ultimately the Check Point Security Gateway (as a VNF)***

NOTE: Chapter 9 provides insights on How Use the Check Point CloudGuard Dome9 Cloud Security Management to implement GANA Knowledge Plane (KP) Security Management-DEs.

The following diagram (Figure 19) presents the capability of Check Point Security Functions to be programmed by specific Knowledge Plane (KP) Platforms responsible for programming the specific Security Functions placed in specific points in the 5G SBA architecture.

NOTE-1: The Check Point security functions shown on the figure apply to both cases, of Horizontal Federation of GANA Knowledge Planes, and Hierarchical Federation of GANA Knowledge Planes Platforms.

NOTE-2: As described earlier, regarding the SBA architecture, the Network Level Security Management-DE in the Knowledge Plane (KP) Platform should also be connected to the GANA Node Level (i.e. the Node-Level (NF-Level)). Meaning it should be connected to a Security Management-DE that may be embedded (as a capability) within each node or be connected to an NF in

general that does not embed a Security Management-DE. Such integration of the SBA functions (e.g. functions in the control plane) with the KP enables to achieve the following objectives:

- at least AMF (to know UE location and to manage UE mobility);
- SMF (to know traffic flow characteristics and to manage flows);
- UDM (to know which NF manage a UE, and manage UE subscription);
- PCF (to manage the policy);
- NRF (to know the load of each NF or a slice and manage NF selection);
- the user plane UPF (to detect certain anomalies such as traffic related anomalies).

The Network Level Security Management-DE in the Knowledge Plane (KP) Platform should also be connected to the NEF (to protect the NEF, which exposes services to an AF (Application Function) and to manage security protection with third party AFs).

[40] presents some examples of some insights on security requirements in the 5G SBA. Also, functions such as the Network Data Analytics Function (NWDAF) [43] [49] and the Management Data Analytics Service (MDAS) [44] need to be integrated with the KP Platform for the core network so that events and KPIs data from the functions can be used by KP DEs in their autonomic operations. Sections 3.2 and 3.3 have already provided some additional insights on the need for the KP platform to leverage the services of NWDAF and/or MDAS.

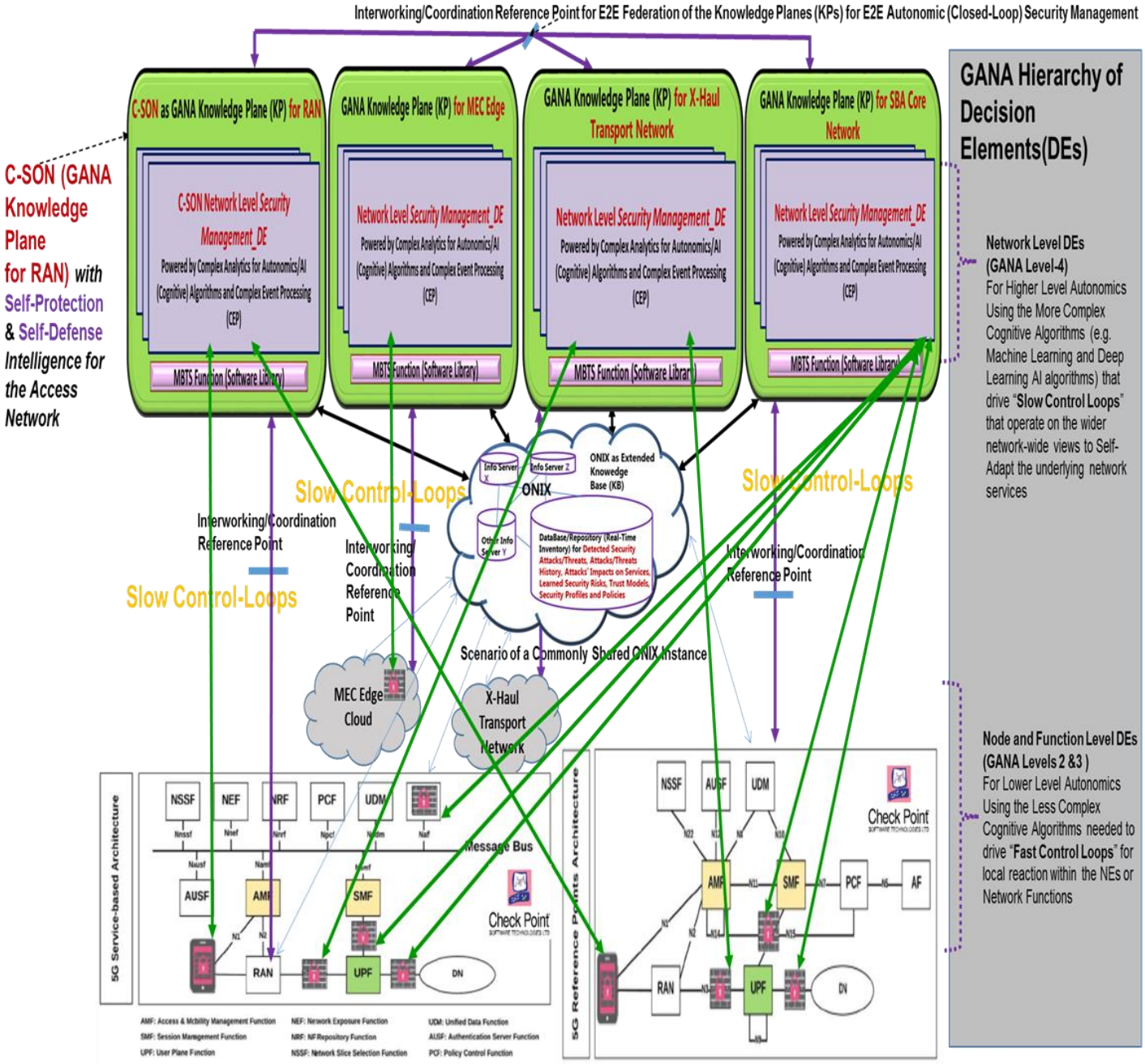

Figure 19: ***The Capability of Check Point Security Functions to be programmed by specific Knowledge Plane Platforms responsible for programming the specific Security Functions placed in specific points in the 5G SBA architecture***

The following diagram (Figure 20) presents the capability to place Check Point Security Platforms (in which Security Functions can be instantiated) at specific security perimeters between network domains, and their capability to be programmed by specific Knowledge Plane Platforms responsible for programming the specific Security Platform and Security Functions instantiated inside the Platform.

NOTE: The Check Point security functions shown apply to both cases of Horizontal Federation of GANA Knowledge Planes and Hierarchical Federation GANA Knowledge Planes.

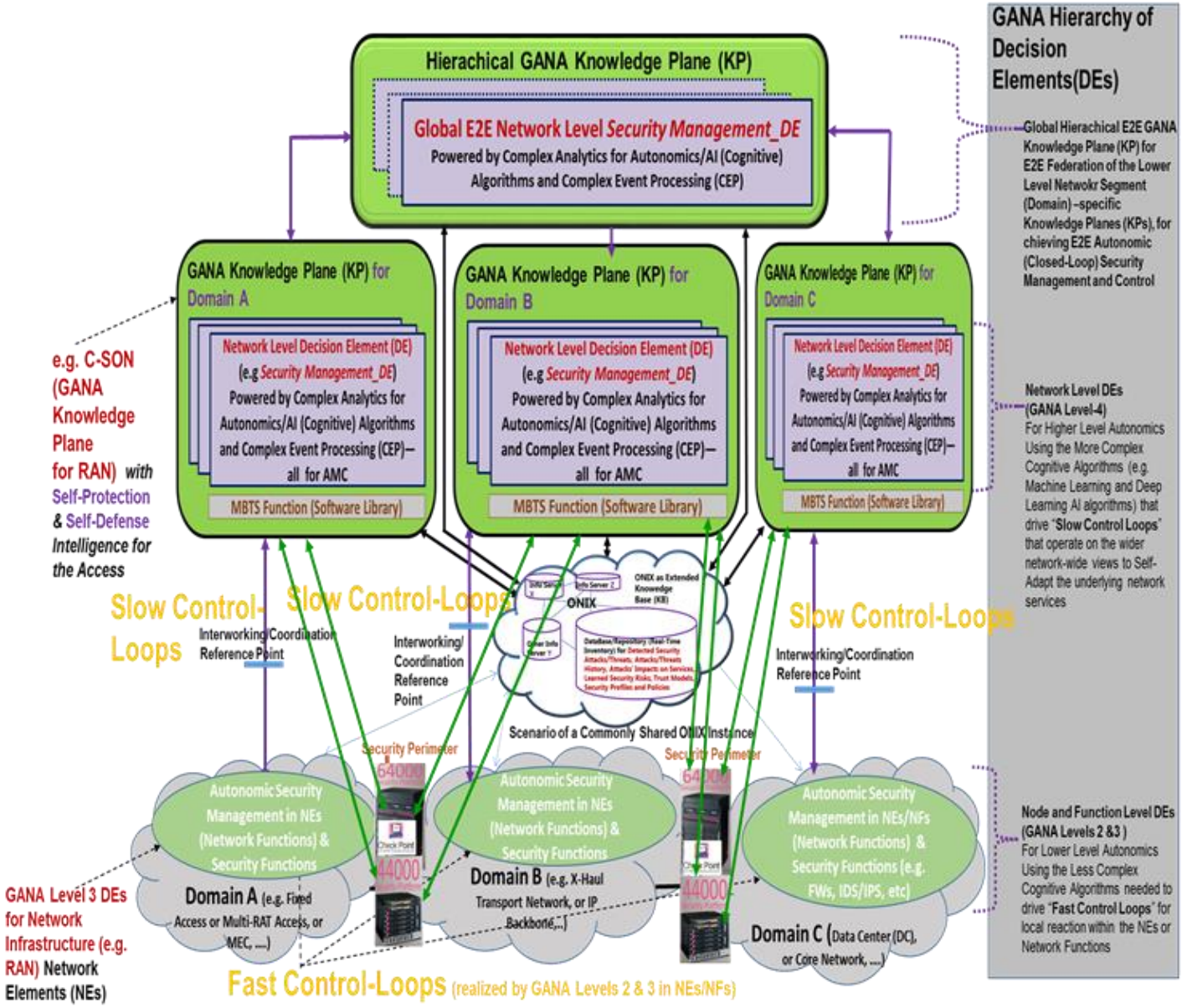

Figure 20: ***The Capability to place Check Point Security Platforms at specific security perimeters between network domains, and their capability to be programmed by specific Knowledge Plane Platforms responsible for programming the specific Security Platform***

The following figures (Figures 21 and 22) present the models of Security Platforms from Check Point that can be used at various security perimeters between domains. There may be some benefits of introducing (implementing) *Fast Control-Loops embedment in Security Functions or Appliances*, although implementing *Fast Control-Loops* in such platforms may not be natively supported by some vendors yet as of today.

Figure 21 presents the flexibility of the Check Point Platforms to enable innovation of GANA Security Management-DE(s), as an AI Model(s), and as a Loadable Module(s) that can be loaded into the Platform and be policy controlled by the KP Level Security Management-DE(s).

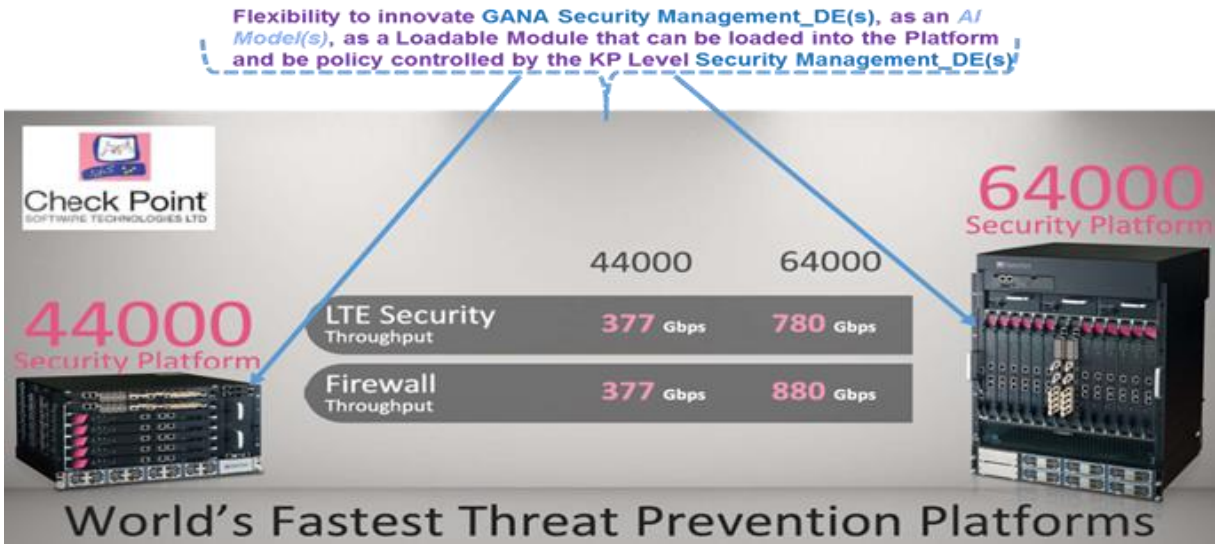

Figure 21: ***The Flexibility of the Check Point Platforms to enable innovation of GANA Security Management-DE(s), as an AI Model(s), and as a Loadable Module(s) that can be loaded into the Platform and be policy controlled by the KP Level Security Management-DE(s)***

Figure 22 presents Other Features of Check Point Threat Prevention Platforms.

Figure 22: ***Other Features of Check Point Threat Prevention Platforms***

Figure 23 presents Check Point Hyperscale Architectures and Integrations with GANA Knowledge Plane (KP) Platforms. Maestro - Hyper Scaling provides for Scale up and down network segments and provides for automated service slicing.

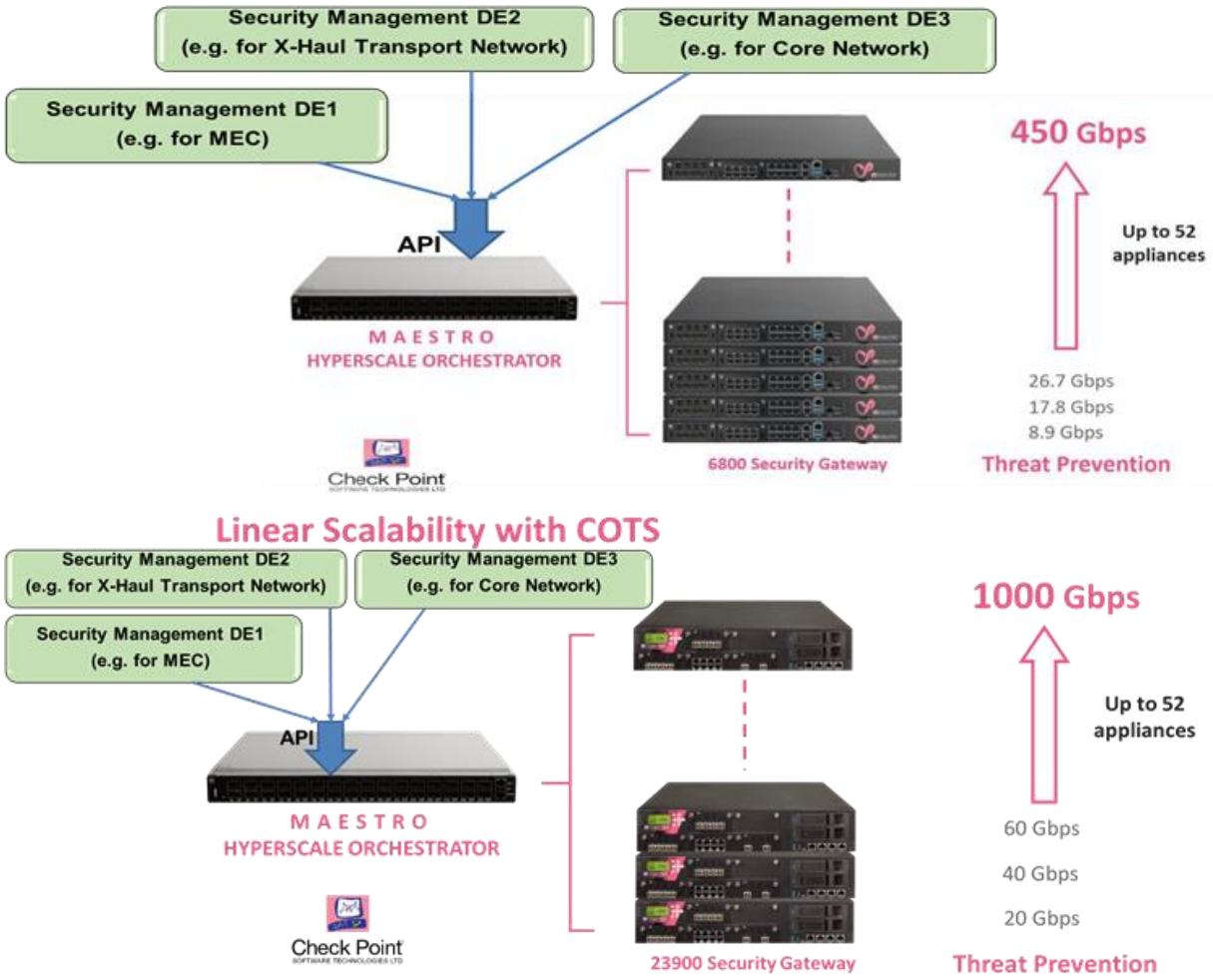

Figure 23: ***Hyperscale Architectures and Integrations with GANA Knowledge Plane (KP) Platforms***

7.3 Other Check Point Capabilities that Address 5G Security Requirements, including 5G Network Security Requirements as per 3GPP TS 33.501

Check Point has various capabilities that address 5G Security Requirements:

- Check Point's Network security solution is architected based on 3GPP TS.33.501
- As part of 3GPP TS 33.501 specification, only encryption and segmentation are the recommended security features which Check Point supports as stated below:
    1. **Section 5.9.1 - Trust Boundaries** → Check Point provides the encryption capabilities as required by the standard
    2. **Section 5.9.2.1 - Security Requirements for service registration, discovery and authorization** → Check Point WAAP solution shall be able to inspect the HTTP/2 messages to ensure compliance to the standard (post 3GPP Rel 16)
    3. **Section 5.9.2.3 - NEF security requirements** → Check Point Dome9 can provide visibility for the communications between the NFs inside a container environment
    4. **Section 5.9.3 - Requirements for e2e core network interconnection security** → Check Point can provide in-network SSL decryption and inspection of malicious HTTP/2 connections as well as limit excessive signaling (per connection)
    5. **Section 9.2, 9.8.2 and 9.8.3 N2/F1/E1 security** → Check Point's IPSEC VPN solution can meet these requirements.

Figure 24 presents 4G/5G parallel Infrastructure Security and Mapping to Check Point Capabilities. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

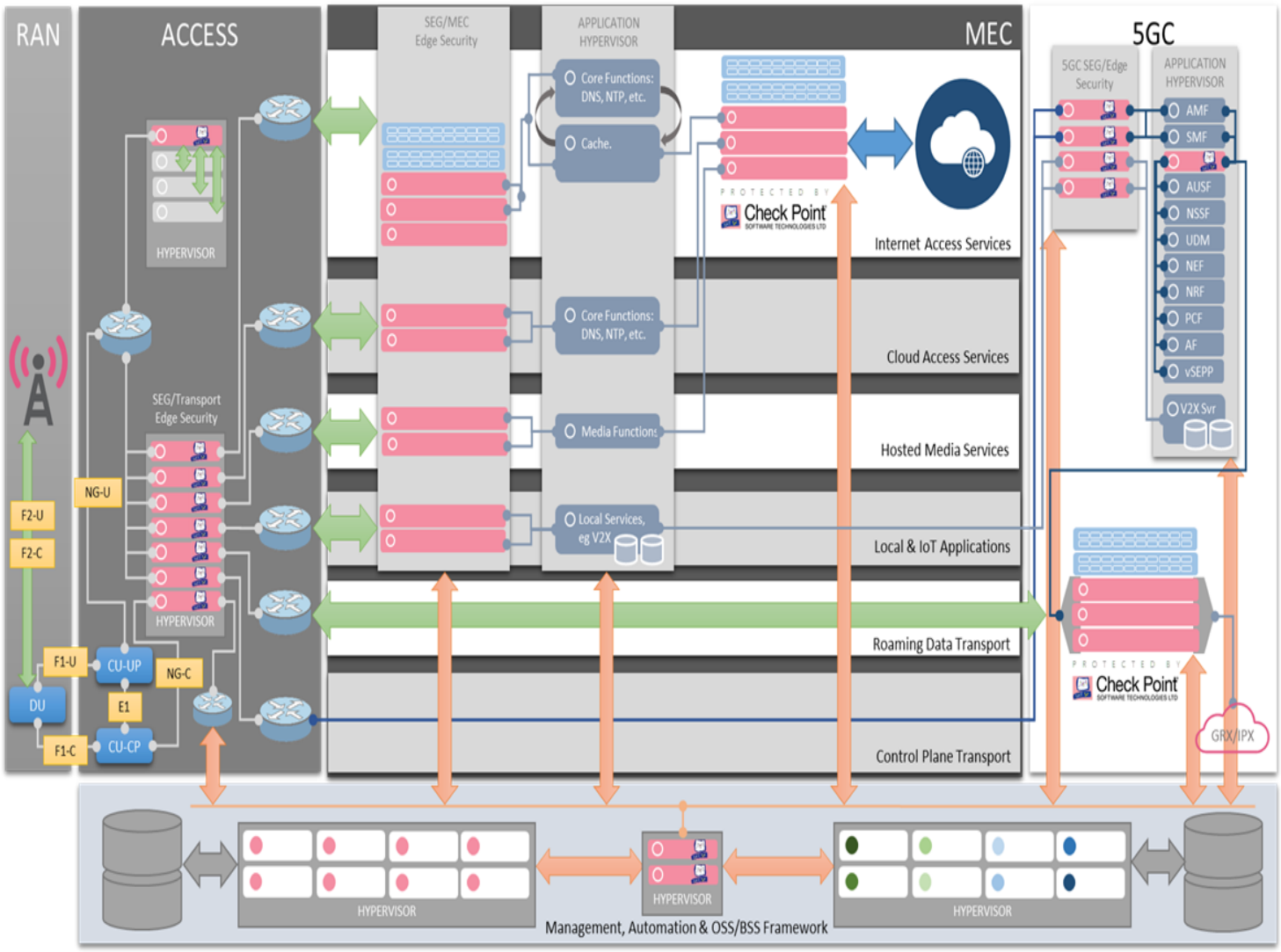

Figure 24: ***4G/5G PARALLEL INFRASTRUCTURE SECURITY and Mapping to Check Point Capabilities***

Figure 25 presents 5G Core (5GC) Security Enforcement Points and Mapping to Check Point Capabilities. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

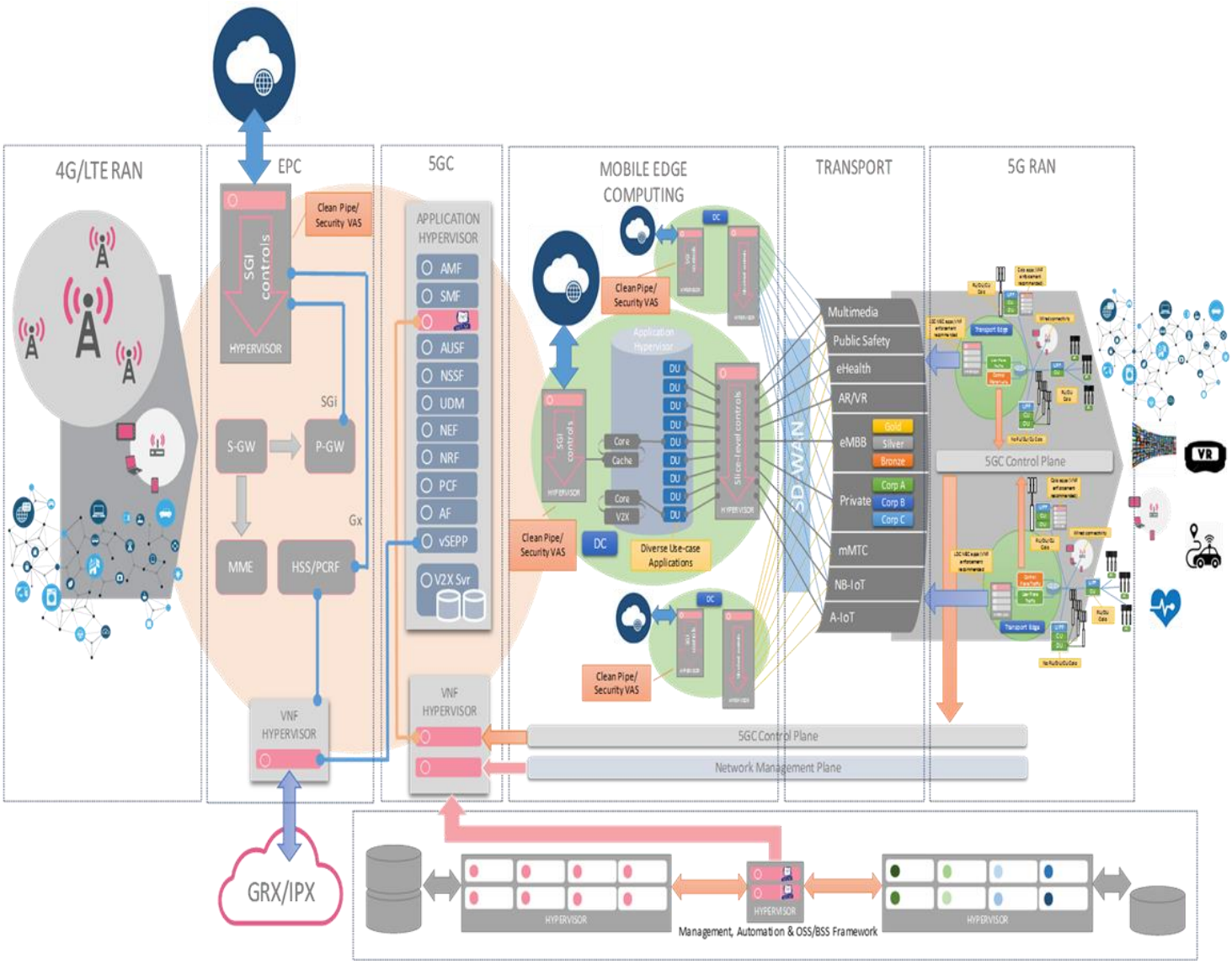

Figure 25: ***5G Core (5GC) Security Enforcement Points and Mapping to Check Point Capabilities***

Figure 26 presents 5G Core Security Enforcement Points and Mapping to Check Point Capabilities. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

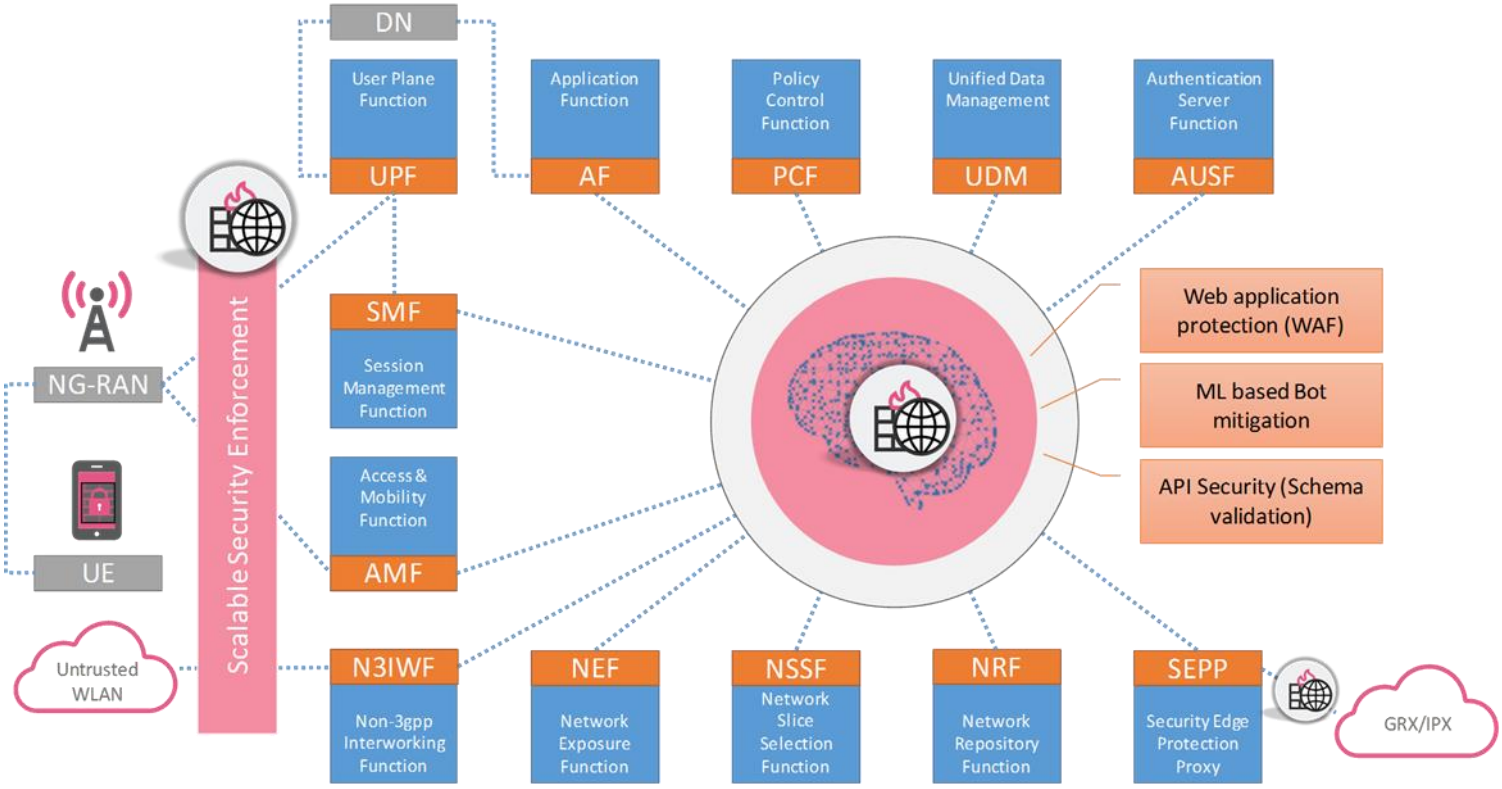

Figure 26: ***5G Core (5GC) Security Enforcement Points and Mapping to Check Point Capabilities***

Figure 27 presents 5G Mobile Network Security Architecture and Check Point capabilities for security enforcement and policing. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

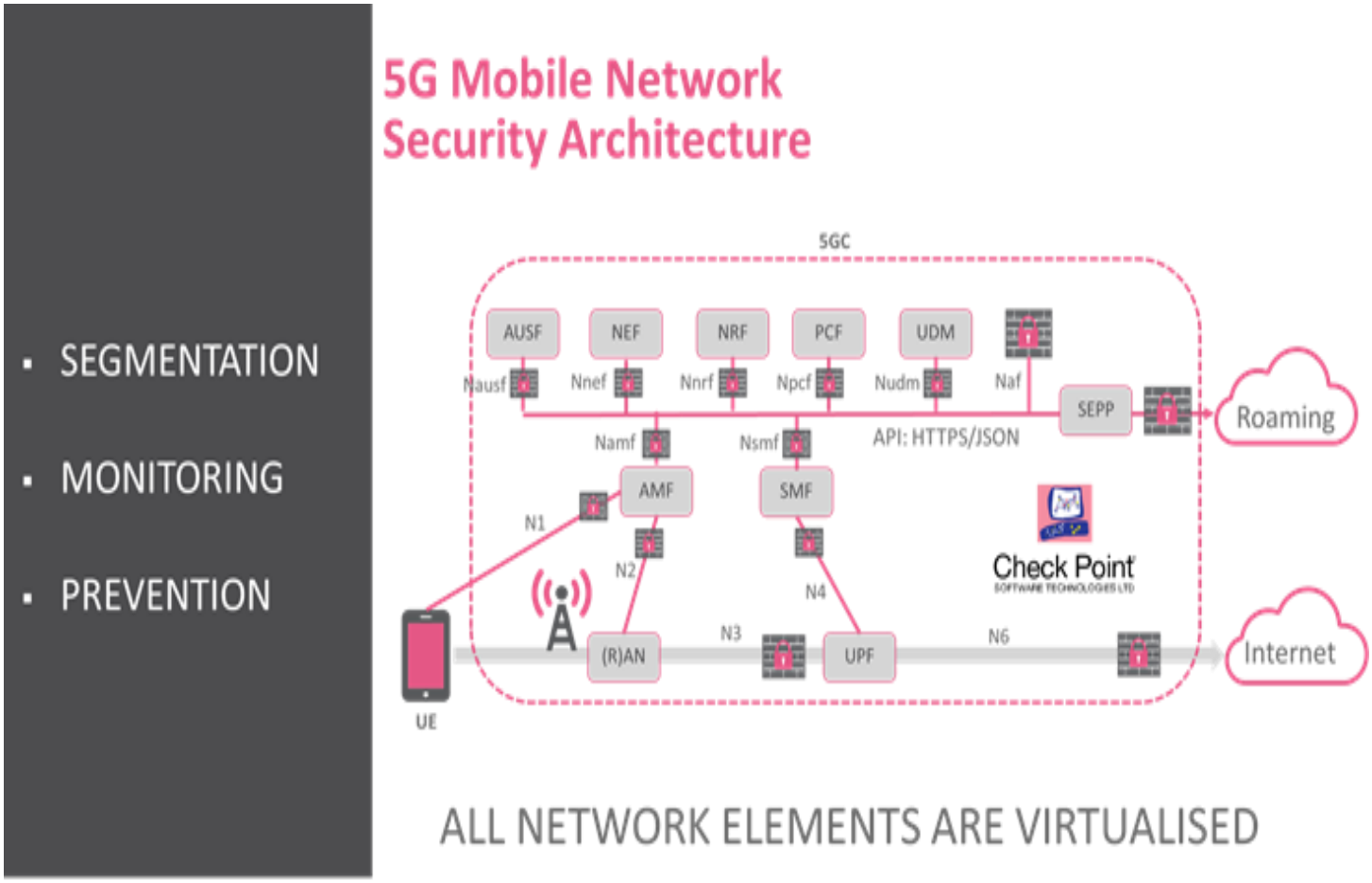

Figure 27: ***5G Mobile Network Security Architecture and Check Point capabilities for security enforcement and policing***

Figure 28 presents Security-as-a-Service (SeCaaS) Use cases (and associated Check Point capabilities). Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

Consumer	▪ Mobile Security-as-a-Service (MSaaS)/Clean Pipe ➢ Consumer Network Security offering using a layered security approach – Network based protection and device based protection
Enterprises/ Government	▪ MSaaS/Clean Pipe for Enterprises ▪ SD-WAN/uCPE/GW-as-a-Service ▪ Managed Network Services ▪ E2E secured communication channels (Government)
IoT	▪ Clean-Pipe for IoT (BOT Mitigation, Device Protection etc.) ▪ Behavioral analysis on the 5G Network

Figure 28: ***Security-as-a-Service (SecaaS) Use cases***

7.4 How to use the Check Point Security Management Platform R80 to implement GANA Knowledge Plane (KP) Security Management-DEs

The following figures (Figure 29, Figure 30, Figure 31, Figure 32 and Figure 33) present Check Point Capabilities that enable to implement GANA Knowledge Plane (KP) Security Management-DEs for specific KPs for specific network segments/domains. Figure 29 presents features of the Check Point Security Management Platform R80 that can be leveraged to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments.

Figure 29: ***Features of the Check Point Security Management Platform R80 that can be used to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments***

Figure 30 presents diversity of the data sources that can be used and correlated in security policies implementations using the Check Point Security Management R80 Platform that can be used to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments.

Figure 30: ***Diversity of the Data Sources that can be used and correlated in security policies implementations using the Check Point Security Management R80 Platform that can be used to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments***

Figure 31 presents Real-Time Event Correlation Capabilities of the R80 Management Platform. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

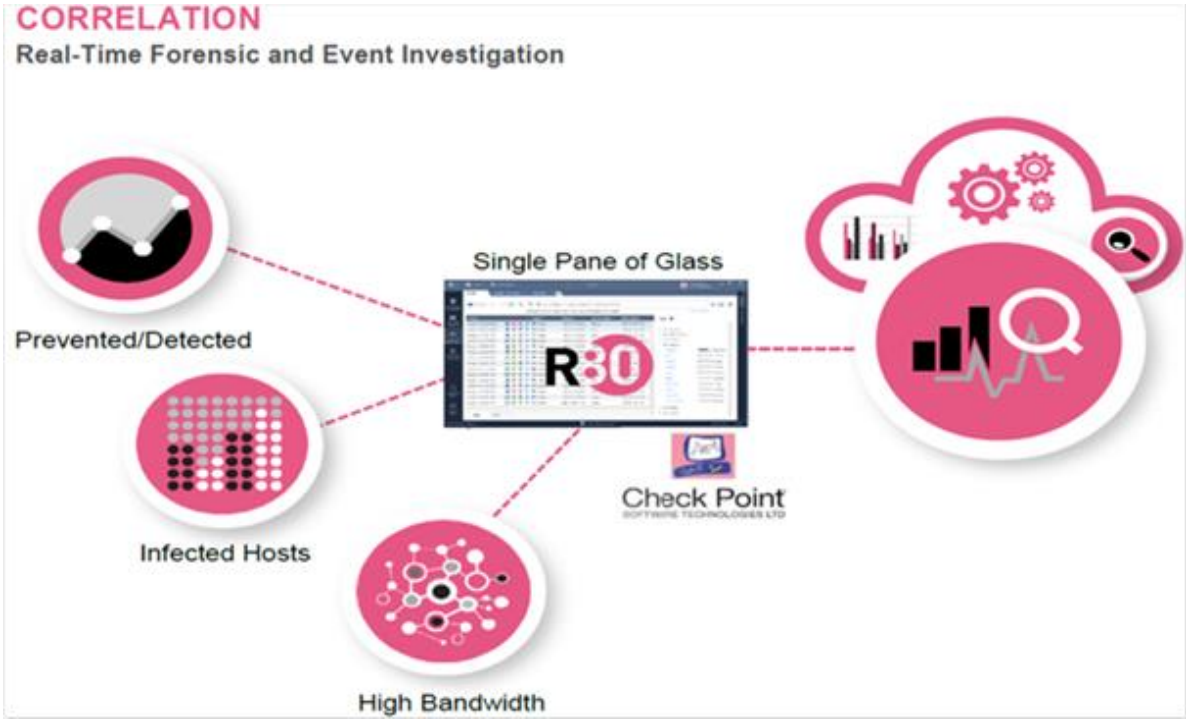

Figure 31: ***Real-Time Event Correlation Capabilities of the R80 Management Platform***

Figure 32 presents various dashboards supported by the Check Point Security Management R80 Platform. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

Figure 32: ***Various Dashboards supported by the Check Point Security Management R80 Platform***

Figure 33 presents the R80 Management API of the Check Point Security Management R80 Platform that can be used in enhancing it with GANA Security Management-DEs (characterized as AI Models that customize the operations of the Check Point Security Management R80 Platform).

Figure 33: ***The R80 Management API of the Check Point Security Management R80 Platform that can be used in enhancing it with GANA Security Management-DEs(characterized as AI Models that customize the operations of the Check Point Security Management R80 Platform)***

Figure 34 presents Example-1 of Reports that the Check Point SmartEvent can produce. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

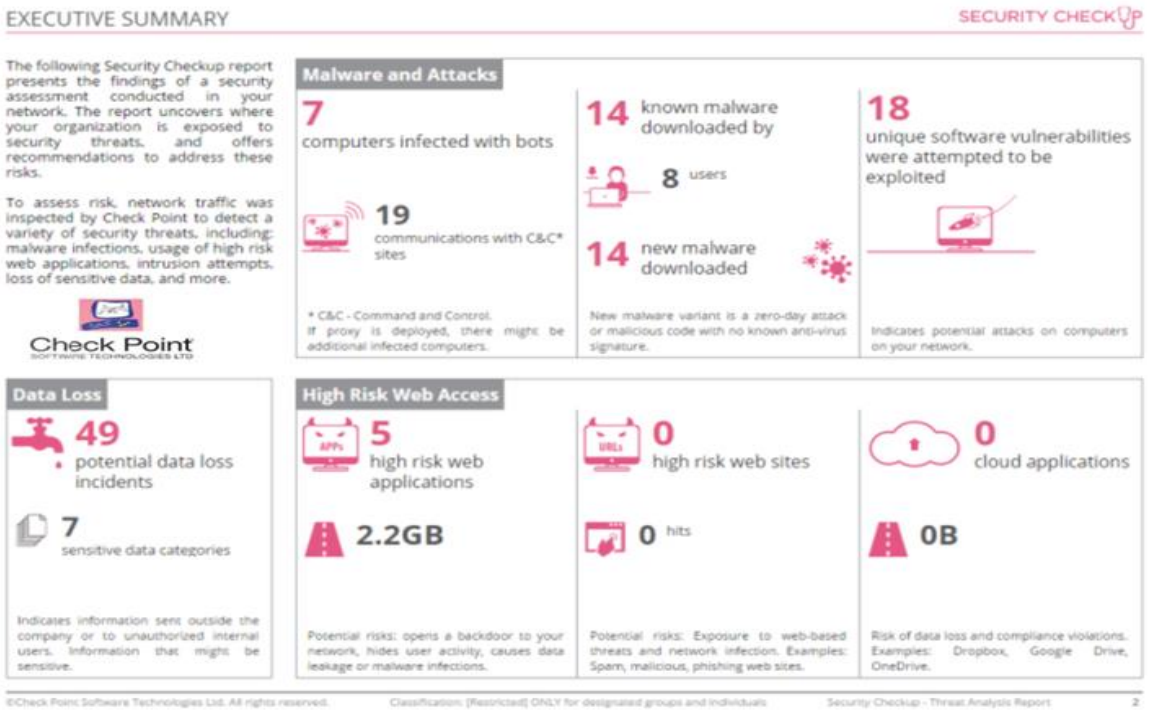

Figure 34: ***Example-1 of Reports that the Check Point SmartEvent can produce***

Figure 35 presents Example-2 of Reports that the Check Point SmartEvent can produce. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

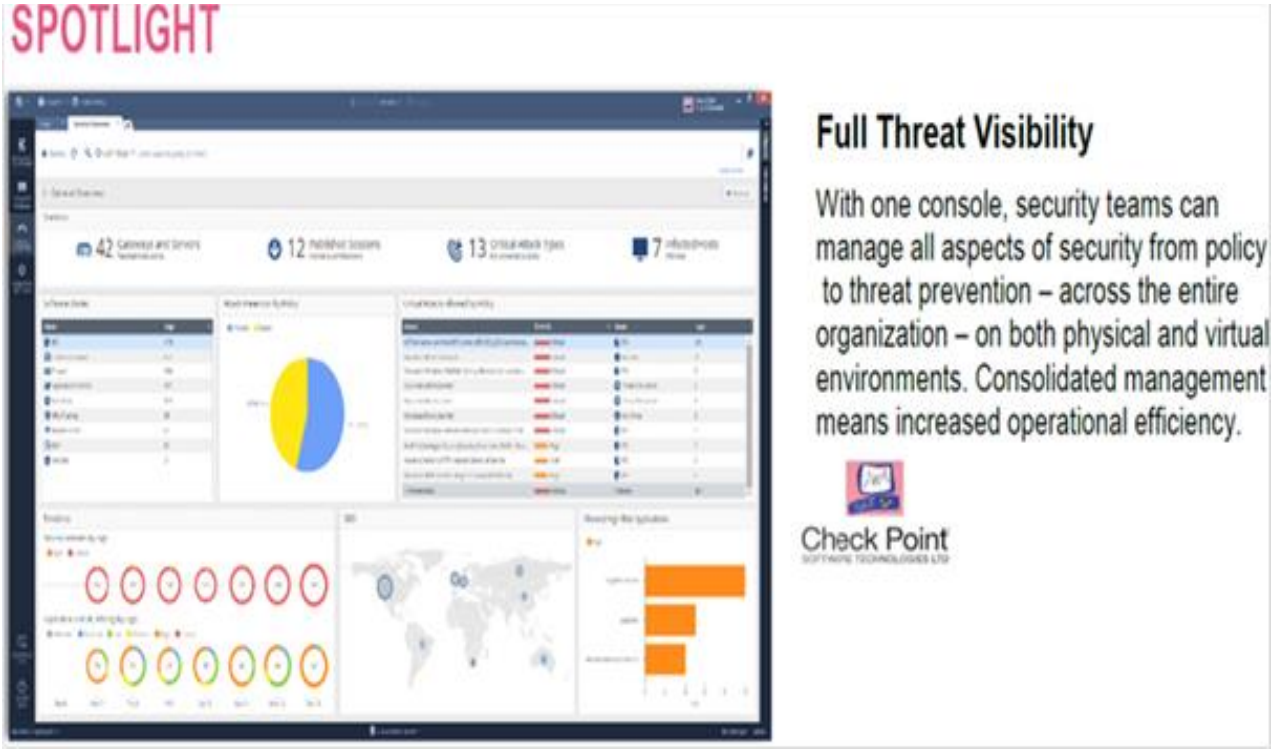

Figure 35: ***Example-2 of Reports that the Check Point SmartEvent can produce***

Figure 36 presents Example-3 of Reports that the Check Point SmartEvent can produce. Implementers of KP Security Management-DEs using Checkpoint security functions and platforms need to take into consideration these capabilities.

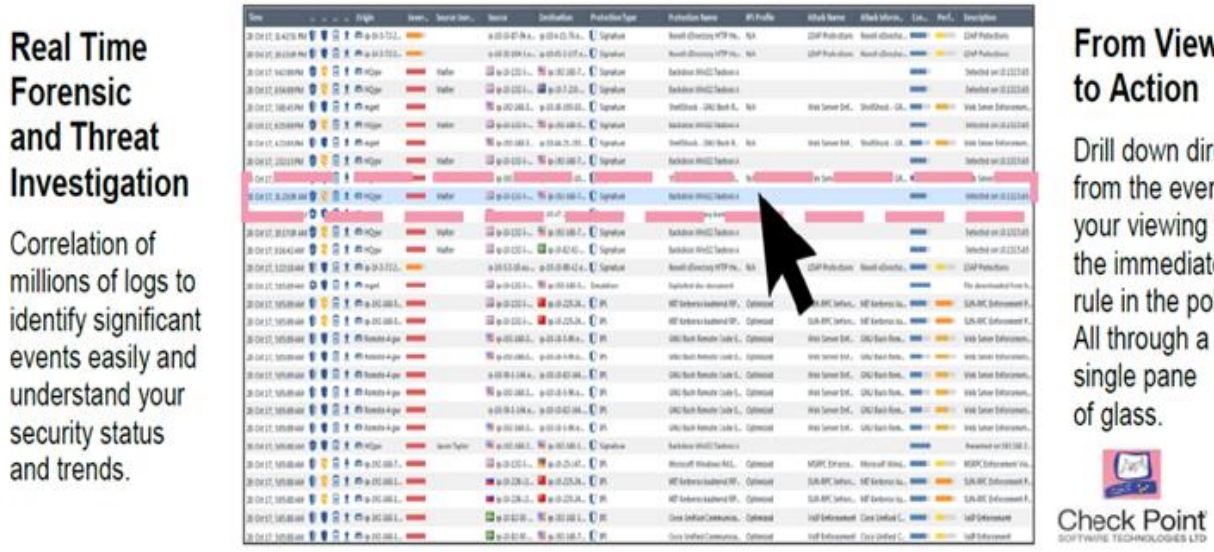

Figure 36: ***Example-3 of Reports that the Check Point SmartEvent can produce***

The following figures (Figure 37 and 38) summarize the Check Point Security Management Platform (R80) that provides for various features of importance to implementing End-to-End Security Policies across various network environments as well as enablers for closed-loop automation in security policy enforcement across various security functions at various points in the network infrastructure. The Check Point Security Management Platform (R80) can be used to implement Security Management DEs of a GANA Knowledge Plane (KP) for a specific network segment, ranging from KP for a MEC edge Cloud, KP for an X-Haul Transport, KP for a Core Network, KP for a general Telco-Cloud, to a KP for a Data Center (DC), as follows:

1. **A KP Level Security Management_DE**, as a deployable AI (Artificial Intelligence) Model, can be implemented ***as a Loadable Module that can be loaded into the Check Point Security Management System***, in a way that can be viewed as customization of the closed-loop security management and control automation capabilities of the Check Point Security Management Platform.
2. Alternatively, a **KP Level Security Management_DE** can be implemented **as an External Entity that drives some operations of the Check Point Security Management System via its API that is already available and exposed to developers** such as developers of KP Level Security Management_DEs, such that the DEs can be implemented as deployable AI (Artificial Intelligence) Models that can be hosted in a different platform than the Check Point Security Management System itself.
3. A single instance of a Check Point Security Management System (Platform) can be used to implement KP Level Security Management_DEs for Multiple GANA Knowledge Planes (KPs), such as KP Level Security Management_DE for MEC Edge Cloud, KP Level Security Management_DE for X-Haul Transport Network, KP Level Security Management_DE for Core Network (Physical or Telco-Cloud), and KP Level Security Management_DE for a Data Center.
4. If a KP Level Security Management_DE is implemented into the Check Point Security Management Platform as a loaded AI Model that customizes the platform as a module, the KP DE-to-KP DE Communication Reference Point of the KP to which the Security Management_DE belongs can be realized as an IP based Network based API that enables the KP's DEs to communicate, because, according to GANA principles, KP DEs interact in exchanging information/knowledge that enable the coordinating DEs to use the information in their decisions on (re)-configuring their respective Managed Entities (MEs). That means the other KP DEs are assumed to be running in a separate Platform from the Check Point Security Management Platform that is hosting the Security Management_DE or Security Management_DEs for various KPs. Figures, Figure 37 and Figure 38, address this case.
5. If a KP Level Security Management_DE is implemented as an External Entity that drives some operations of the Check Point Security Management System via its API that is exposed to developers of a KP Level Security Management_DEs (as deployable AI (Artificial Intelligence) Models that can be hosted in a different platform than the Check Point Security Management System itself), then the KP DE-to-KP DE Communication Reference Point of the KP to which the Security Management_DE belongs can be realized as local API of the host platform (not the Check Point Platform) for the KP DEs (including the Security Management-DE), or it may be realized as an IP based Network based API that enables the KP's DEs to communicate (as illustrated on Figure 37 and Figure 38). This is because, according to GANA principles, KP DEs interact in exchanging information/knowledge that enable the coordinating DEs to use the information in their decisions on (re)-configuring their respective Managed Entities (MEs). That means all the KP DEs (including the Security Management_DE) are assumed to be running in separate Platform from the Check Point Security Management Platform.

Figure 37 presents the Capability of using the Check Point Security Management Platform R80 to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments.

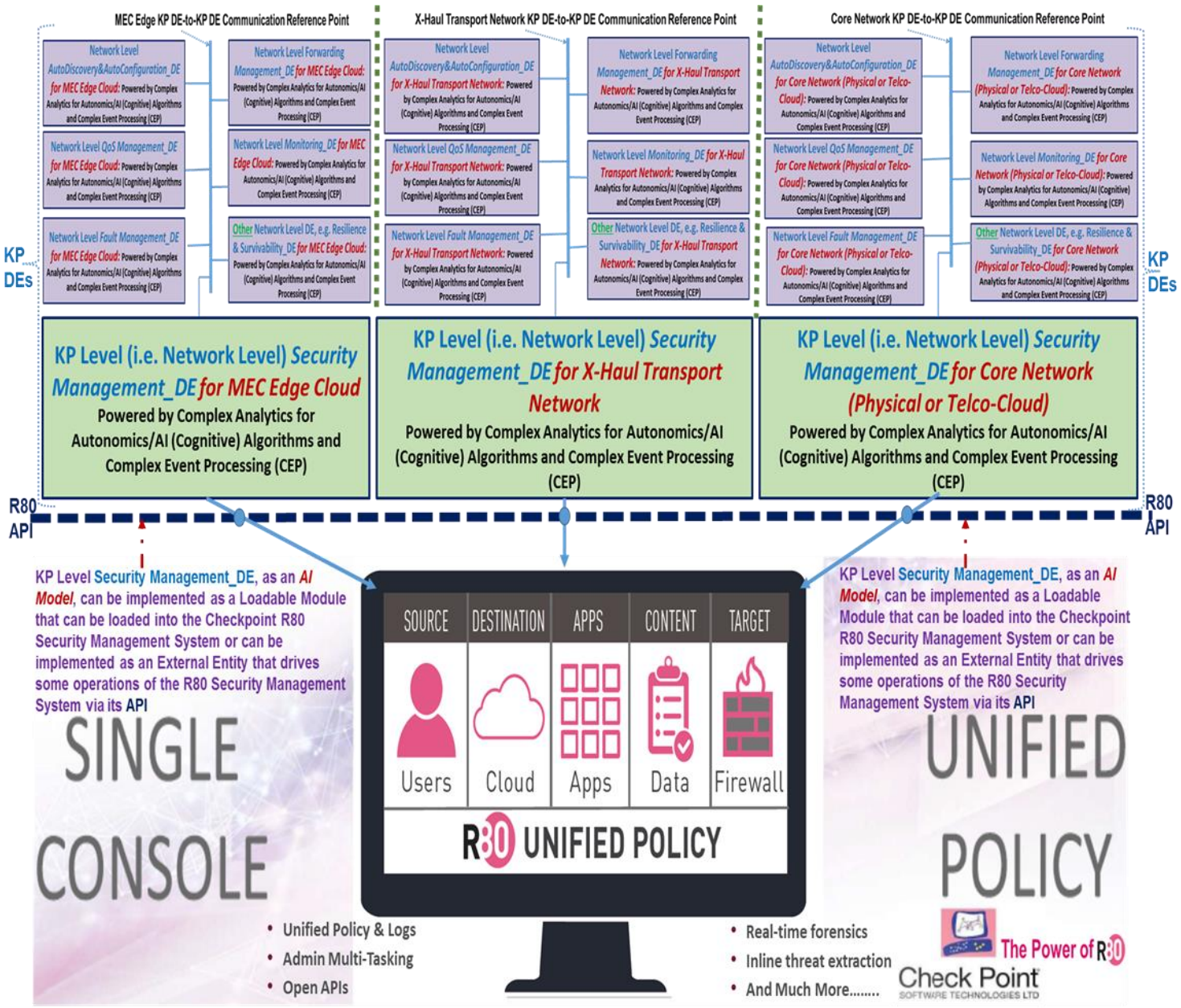

Figure 37: ***Using the Check Point Security Management Platform R80 to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments***

Figure 38 presents the Capability of using the Check Point Security Management Platform R80 to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments. In addition, the figure presents the capability of using an IP based Network API (Application Programming Program) to enable the other DEs (apart from the Security Management-DE) belonging to the same Knowledge Plane Platform for a specific network segment and yet hosted in a different environment than the R80 to communicate with the Security Management-DE of the same KP Platform. This is in reference to a Security Management-DE that is considered as having been implemented on the R80 platform.

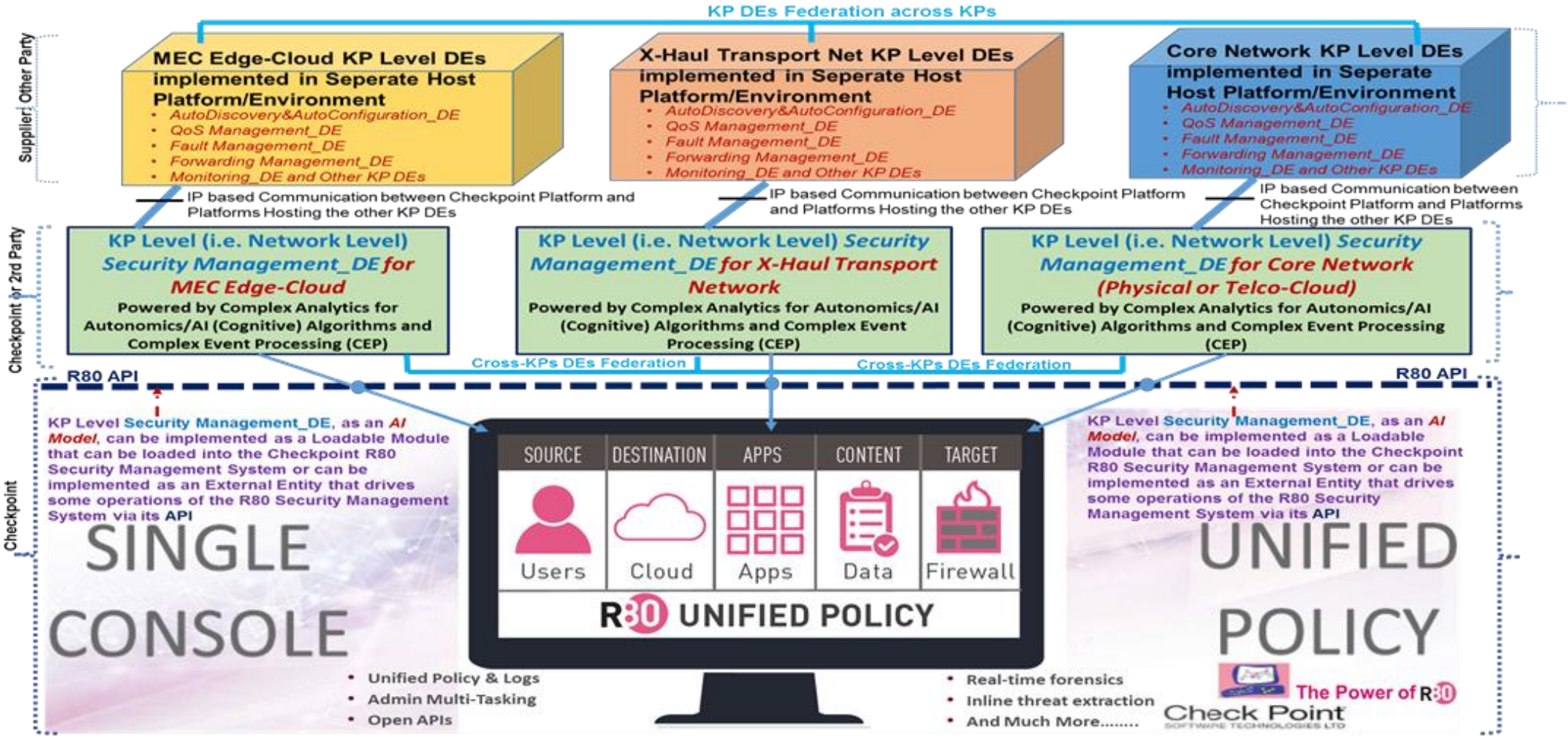

Figure 38: Using the Check Point Security Management Platform R80 to implement Security Management-DEs of ETSI GANA Knowledge Planes for specific Network Segments

8. Further Illustrations on Implementing a GANA KP Level Security Management DE using the Check Point R80 Platform Environment and its Data Lake

The Chapter 5 on "Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection and Threats/Risks Predictions", presented useful insights on how to implement a Security Management-DE that operates on the level of a GANA Knowledge Plane (KP) as one of the DEs of a KP platform, with illustration provided by Figure 16. This present chapter provides additional insights in reference to the guidelines provided in chapter 7 on how to implement a Security Management-DE using the capabilities of the Check Point R80 management platform. As illustrated on Figure 39, this section presents the Check Point R80 Capabilities that can be used to implement a Security Management-DE for a Knowledge Plane Platform. This is considered in combination with an implementation of a Check Point's THREATCLOUD capability of value to implementing a ***DataBase/Repository (Real-Time Inventory) of the ONIX that stores Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies*** as part of an ONIX system. Figure 39 presents the capability of using the Check Point Security Management R80 Platform to Implement a GANA KP Level Security Management DE for Open/Closed-Loop Correlation and Autonomic Security Management & Control (in highlighting Check Point specific capabilities to the Figure 16 in Chapter 5). That means implementers of a Security Management-DE should also consider the Check Point capabilities described in chapter 7, such as Check Point capabilities described in section 7.1, section 7.2, section 7.3 and section 7.4. In addition, the Figure 39 shows that the **Check Point R80 Management Platform implements a Data Lake** that can be used by a Security Management-DE. This is because, as mentioned in Chapter 5, various Data that may be available through a Data Lake may be of interest to the Security Management-DE to consume in form of the raw data or in form of knowledge that may be synthesized by Data Analytics/AI algorithms running on the Data Lake. As discussed in section 7.2, Check Point capabilities include security functions that can be dynamically orchestrated using a MANO stack and instantiated in a virtualized environment by a Security Management-DE during its autonomic operations and in strategies on handling detected and/or predicted security attacks and threats on the underlying network infrastructure and services being delivered by the network.

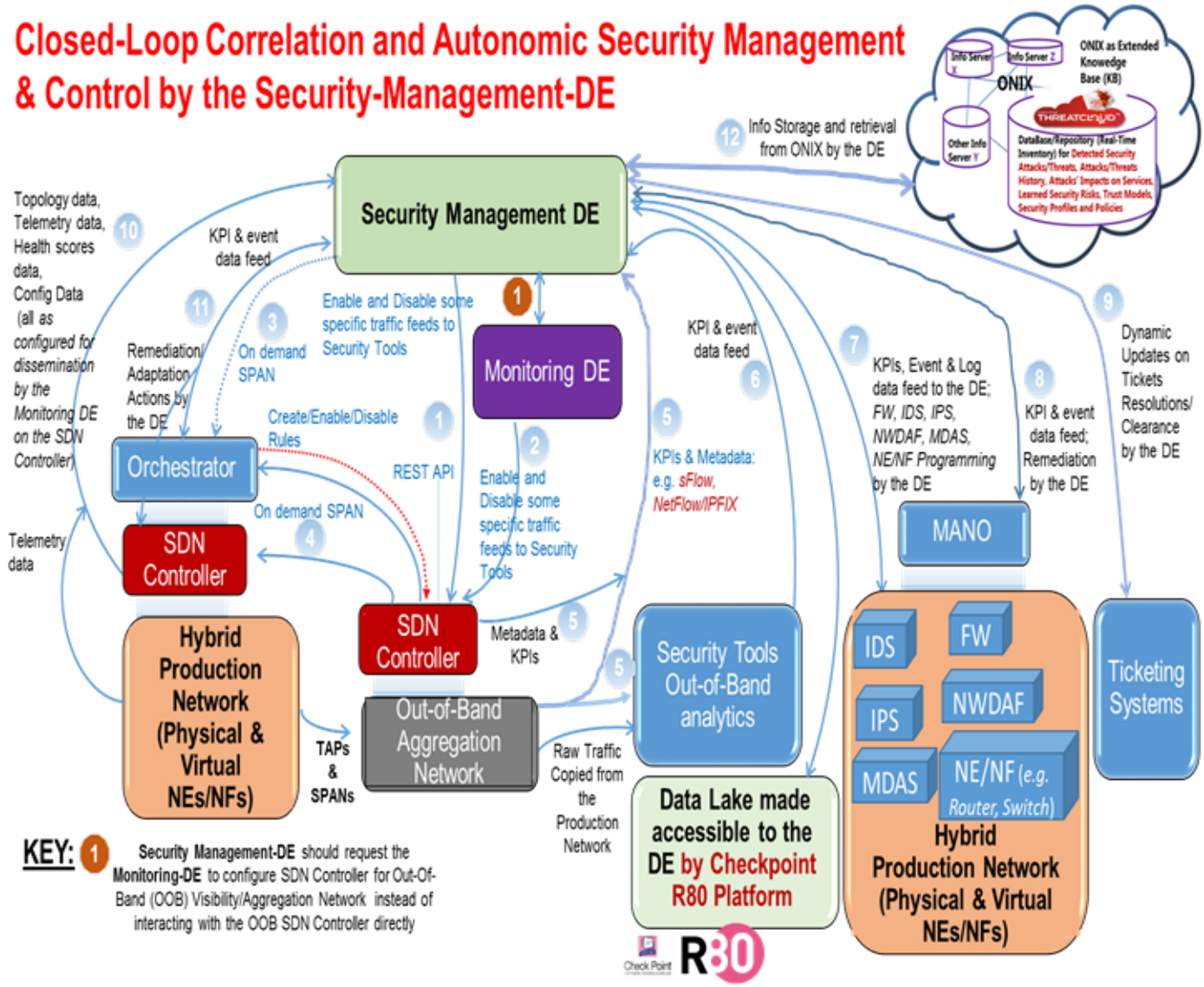

Figure 39: ***Using the Check Point Security Management R80 Platform to Implement a GANA KP Level Security Management DE for Open/Closed-Loop Correlation and Autonomic Security Management & Control***

9. Using the Check Point CloudGuard Dome9 Cloud Security Management to implement GANA Knowledge Plane (KP) Security Management-DEs

Section 7.3 covered the subject of "How to use the Check Point Security Management Platform (R80) to implement GANA Knowledge Plane (KP) Security Management-DEs". This chapter provides a glimpse of another Check Point Security Management Platform that can be used to implement KP Security Management DEs, but in a Cloud Environment, for Cloud Security Management. Figure 40 presents the possibility of KP Security DEs implementation in a Cloud Environment using the CloudGuard Dome9 Cloud Security Management.

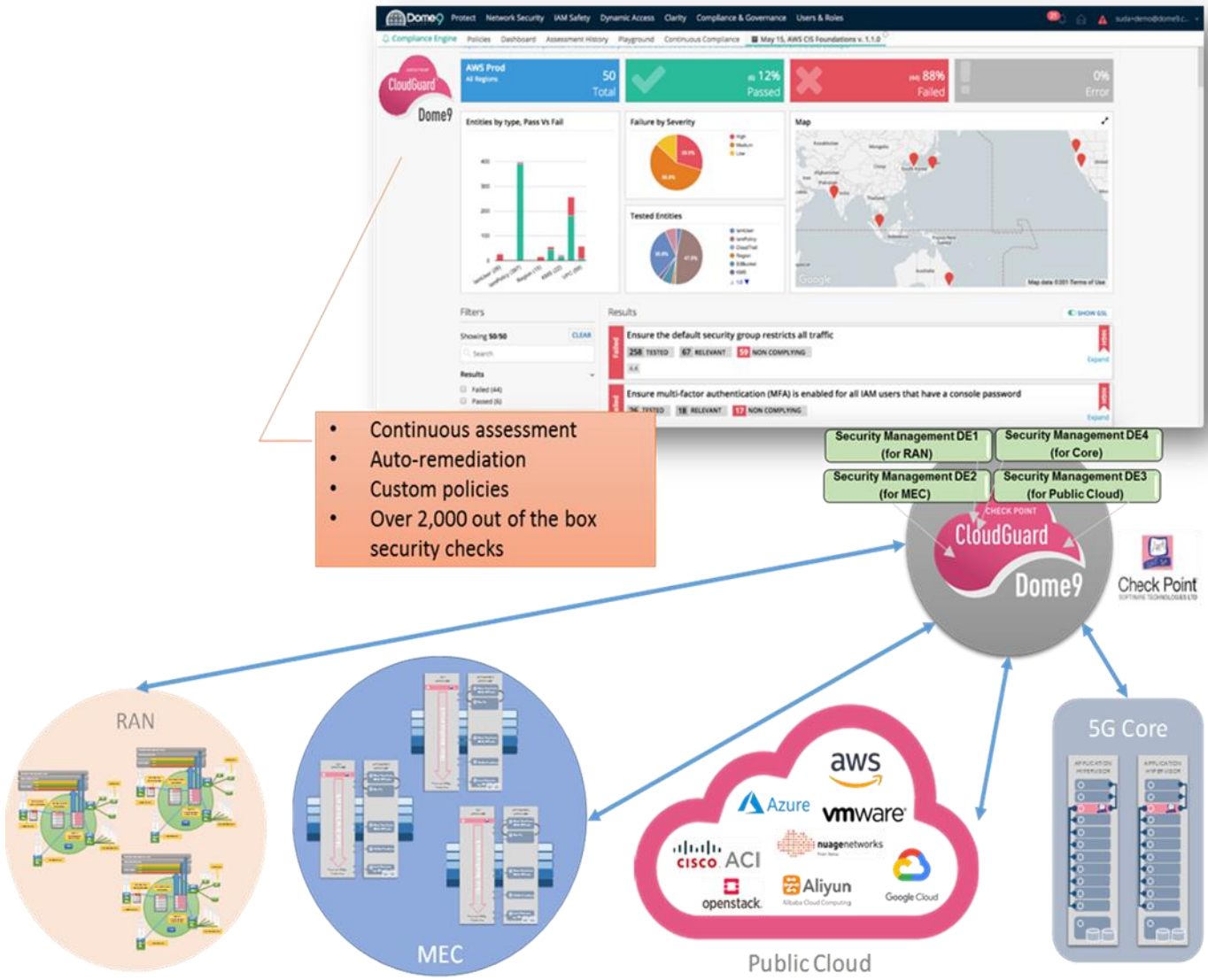

Figure 40: KP Security DEs implementation in a Cloud Environment using the *CloudGuard Dome9 Cloud Security Management*

10. Conclusions on what should be targeted for Standardization of the Generic Framework for E2E Autonomic (Closed-Loop) Security Management & Control for 5G Networks

This White Paper has been written to lay the groundwork for standardization work that can be launched in ETSI TC INT on Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services, as concluded in this paper. Such target Specification should cover the definition of the Generic Framework in more detail and also the "Information" that need to be exchanged on a Federation Reference Point(Rfp) for Knowledge Plane to Knowledge Plane Federations, as well as the *Messages and Communication Means* that should be standardized (e.g. in ETSI TC INT AFI WG). Additional Items that can be standardized include the following:

- The Information that should be exchanged on the "KP DE"-to- "KP DE" Reference Point (Rfp) concerning DEs that belong to the same Knowledge Plane (KP) Platform, and the communication means (e.g. messages) that can be used by the DEs. These may also be standardized especially if KP DEs may be supplied by different players to a KP Platform builder, integrator or supplier.
- In considering the concept of "***Market Place for AI Models and DEs for AMC***" for sourcing of AI-powered DEs of differentiated quality of decision-making for AMC, described in [22], then standardization of the "primitives" and "information" that can be used in DE-to-DE communications (*e.g. "Security Management-DE" to "Monitoring-DE"; or "Security Management-DE" to "QoS Management-DE"*) is desirable. Because this also enables innovation in AI models and DEs.

NOTE1: The work on standardizing such items must build on the definitions of GANA Reference Points (Rfps) and associated Characteristic Information exchange as defined in ETSI TS 103 195-2 and in various GANA instantiations. GANA instantiations such as GANA instantiation onto BroadBand Forum (BBF) architectures (ETSI TR 103 473 V1.1.2), GANA instantiations onto the 3GPP Backhaul and Core Network (ETSI TR 103 404)) and other GANA instantiations documents produced by ETSI (e.g. ETSI TR 103 626 and ETSI TR 103 495).

NOTE2: Readers are encouraged to follow the developments in ETSI on the standardization of the Framework presented in this White Paper, namely the "***Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Networks/Services***", and join those standardization efforts.

11. References

[1] ETSI White Paper no. 16: The *Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services*: http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp16_gana_Ed1_20161011.pdf

[2] ETSI TS 103 195-2 (published by ETSI in May 2018): Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; **Part 2:** ***An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management***: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=50970

[3] ETSI 5G PoC on 5G Network Slices Creation, Autonomic & Cognitive Management & E2E Orchestration—with Closed-Loop (Autonomic) Service Assurance for the IoT (Smart Insurance) Use Case: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals

[4] 5G security recommendations: Package #2: Network Slicing, by NGMN Alliance: 27-April-2016,

[5] White Paper No.1 of the ETSI 5G PoC: C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals

[6] ODA TM Forum's Open Digital Architecture (ODA): IG1167 ODA Functional Architecture Vision R18.0.0 (Intelligence Management Function Block)

[7] ETSI TR 103 473 V1.1.2: Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures: GANA Autonomics in BBF Architecture Scenarios

[8] ETSI TR 103 404: GANA instantiation onto the 3GPP Backhaul and Core Network architectures

[9] ONAP Open Source Project: ONAP Architecture Overview: https://www.onap.org/

[10] 5G security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience: by NGMN Alliance: 20 February 2018, by NGMN 5G security group

[11] BBF CloudCO Open Source Project: https://www.broadband-forum.org/cloudco

[12] OPNFV Open Source Project: https://www.opnfv.org/

[13] ONOS Open Source Project: https://onosproject.org/

[14] OpenDayLight Open Source Project: https://www.opendaylight.org/

[15] ETSI OSM (Open Source MANO): https://osm.etsi.org/

[16] ACUMOS: An Open Source AI Machine Learning Platform: https://www.acumos.org/

[17] White Paper No.3 of the ETSI 5G PoC: Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals
[18] ODA TM Forum's Open Digital Architecture (ODA): IG1177 ODA Intelligence Management Implementation Guide: R18.5.0 (IG1177 Release 18.5, December 2018)
[19] White Paper No.2 of the ETSI 5G PoC: ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON – ONAP Architecture: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals
[20] James Crawshaw: Network Automation Roadmap: Where to Start & What to Aim for: A Heavy Reading white paper produced for Juniper Networks Inc.
[21] Cabaj K., Szczypiorski K., Becker S. (2010) Towards Self-defending Mechanisms Using Data Mining in the EFIPSANS Framework. In: Nguyen N.T., Zgrzywa A., Czyżewski A. (eds) Advances in Multimedia and Network Information System Technologies. Advances in Intelligent and Soft Computing, vol 80. Springer, Berlin, Heidelberg: DOI: 10.1007/978-3-642-14989-4_14
[22] White Paper No.4 of the ETSI 5G PoC: ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals
[23] Alberto Huertas, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martinez Perez: Towards the autonomous provision of self-protection capabilities in 5G networks: December 2019: Journal of Ambient Intelligence and Humanized Computing 10(12):4707-4720: DOI: 10.1007/s12652-018-0848-6
[24] Manuel Gil Perez, et al: Self-Organizing Capabilities in 5G Networks: NFV & SDN Coordination in a Complex Use Case: EuCNC 2018-3rd Network Management Workshop for 5G Networks, June 2018
[25] 5G End-to-End Architecture Framework by NGMN Alliance: P1-Requirements and Architecture: NGMN 5G E2E Architecture Framework v3.0.8: https://www.ngmn.org/publications/5g-end-to-end-architecture-framework-v3-0-8.html
[26] ETSI 5G PoC Report on Specifications of Integration APIs for the ETSI GANA Knowledge Plane Platform with Other Types of Management & Control Systems, and with Info/Data/Event Sources in general: https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals
[27] Ashutosh Dutta, Ph.D.: Conference Slides: Security in SDN/NFV and 5G Networks Opportunities and Challenges: Chair, IEEE Future Network Initiative: 05/06/2019.
[28] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov: 5G Security: Analysis of Threats and Solutions: In 2017 IEEE Conference on Standards for Communications and Networking (CSCN): DOI: 10.1109/CSCN.2017.8088621
[29] Palo Alto Networks White Paper: 5G SECURITY: Establishing a Holistic Approach to Paving the 5G Evolution: 2018
[30] Falko Dressler, Gerhard Münz, Georg Carle: Attack detection using cooperating autonomous detection systems (CATS): Proceedings of 1st IFIP International Workshop on Autonomic Communication, Poster Session, Berlin, Germany, October 2004
[31] Anastasios Zafeiropoulos, Athanassios Liakopoulos, Alan Davy, Ranganai Chaparadza: Monitoring within an Autonomic Network: A GANA Based Network Monitoring Framework: Conference: Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops - International Workshops, ICSOC/ServiceWave 2009, Stockholm, Sweden, November 23-27, 2009, Revised Selected Papers: DOI: 10.1007/978-3-642-16132-2_29
[32] On Using sFlow for Security Attacks detection: https://inmon.com/pdf/sFlowSecurity.pdf ; https://sflow.org/using_sflow/
[33] Cisco White Paper: Network as a Security Sensor White Paper: October 26, 2018: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.pdf
[34] Flowmon White Paper "Whitepaper – Flow for Security: IP flow based detection of cyber threats", and online article: Network Behavior Analysis & Anomaly Detection: https://www.flowmon.com/getattachment/9f4bed3b-a5ba-4a32-af98-c65658a8e14e/IP-Flow-

Based-Detection-of-Cyber-Threats.aspx; https://www.flowmon.com/en/solutions/security-operations/network-behavior-analysis-anomaly-detection

[35] Anna Sperotto: PhD Thesis: Flow-Based Intrusion Detection: 2010: https://annasperotto.org/thesis/thesis.pdf

[36] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller: An Overview of IP Flow-Based Intrusion Detection: IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 3, THIRD QUARTER 2010

[37] Jordan Lam, Robert Abbas: Machine Learning based Anomaly Detection for 5G Networks: March 2020, https://arxiv.org/abs/2003.03474

[38] Jiaqi Li, Zhao Zhifeng, Rongpeng Li: A Machine Learning Based Intrusion Detection System for Software Defined 5G Network: DOI: 10.1049/iet-net.2017.0212

[39] European Union Agency for Network and Information Security (ENISA) Publication on THREAT LANDSCAPE FOR 5G NETWORKS: Threat assessment for the fifth generation of mobile telecommunications networks (5G): NOVEMBER 2019

[40] White Paper by Huawei: Partnering with the Industry for 5G Security Assurance: https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf

[41] GSMA Report: AI in Network Use Cases in China: October 2019: https://www.gsma.com/futurenetworks/wp-content/uploads/2019/10/AI-in-Networks-Use-Case-V.03-231019-Document.pdf

[42] Andrea Peiro, CUJO AI: Securing 5G Networks With Deep Learning-Based Threat Detection Systems: by Blogs & Opinions 6/10/2019 https://www.the5gexchange.com/author.asp?section_id=743&doc_id=752076

[43] ETSI TS 129 520 V15.0.0 (2018-07): 5G; 5G System; Network Data Analytics Services: Stage 3: (3GPP TS 29.520 version 15.0.0 Release 15)

[44] ETSI TS 128 533 V15.0.0 (2018-10): 5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)

[45] White Paper by Huawei: AI Security White Paper: 2018

[46] Kelsey Ziser, Jim Hodges, Gordon Mansfield, Christina Ashraf: Article: 5G Exchange: eBook: Innovation at the Speed of 5G

[47] JIM HODGES, Heavy Reading White Paper, 2019: Implementing 5G Security: Priorities and Preferences: A Heavy Reading white paper produced for F5 Networks, Fortinet, NetNumber, and Palo Alto Networks:

[48] Verizon White Paper: Network Threat Advanced Analytics: 2016

[49] 3GPP: Architecture enhancements for 5G System (5GS) to support network data analytics services: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579

[50] Online Article by RCR Wireless News: How to develop 5G security standards at a global scale: https://www.rcrwireless.com/20200120/5g/how-to-develop-5g-security-standards-at-a-global-scale

[51] Emmanouil Pateromichelakis, et al: End-to-End Data Analytics Framework for 5G Architecture: In IEEE Access Online SPECIAL SECTION ON ROADMAP TO 5G: RISING TO THE CHALLENGE, VOLUME 7, 2019:

[52] White Paper No.5 of the ETSI 5G PoC: *Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation:* https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals

[53] 3GPP SA3 - Security: https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

[54] ETSI GS NFV-SEC 013: Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification

[55] ETSI GS NFV-REL 004: "Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection"

Editors of the White Paper, and Main Contact

ETSI World Class Standards

ETSI 5G PoC Consortium Steering Committee and Contributors:

- *Tayeb Ben Meriem, PhD: Orange: Senior Standardization Manager & Technical Expert: ETSI TC-INT/AFI WG Chair; PoC Steering Committee Member; France*
- *Ranganai Chaparadza, PhD: Altran Germany: Technical Expert & Senior Consultant/Vodafone Consultant; IPv6 Forum; PoC Steering Committee Member; Germany*
- *Eugen Hinz, Security Solutions Engineer-Telco, Check Point Software Technologies GmbH, Germany*
- *Aviv Abramovich, Security Solutions Architect, R&D, Check Point Software Technologies, Israel*
- *Michael Stichel, Head of Telco EMEA, Check Point Software Technologies GmbH, Germany*
- *Chris Federico, Security Solutions Architect, R&D, Check Point Software Technologies, Israel*
- *Eli Morinies, Security Solutions Architect, R&D, Check Point Software Technologies, Israel*
- *Shay Naveh, Security Solutions Architect, R&D, Check Point Software Technologies, Israel*
- *Benoit Radier, PhD: Orange: Standardization & Technical Expert; PoC Steering Committee Member; France*
- *Muslim Elkotob, PhD: Vodafone: Technical Expert and Solutions Design Architect & Standardization Expert; Germany*
- *Ralf Karbstein; Testing Expert; Senior Account Manager at DATAKOM; Germany*
- *Said Soulhi, PhD: Verizon: Technical Expert and Solutions Design Architect & Standardization Expert; PoC Steering Committee Member*
- *Takayuki Nakamura: NTT: Technical Expert and Solutions Design Architect & Standardization Expert; Japan*
- *Giulio Maggiore: Telecom Italia: Core, Transport & Service Platforms Engineering & Development, Fixed & Mobile Core Network: Standardization Expert: ETSI TC-INT Chair; Italy*

ETSI INT 5G PoC wiki: http://ntechwiki.etsi.org/; https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals:

5G PoC Leader and INT AFI WG Chairman: Tayeb Ben Meriem (Orange)
tayeb.benmeriem@orange.com

Acknowledgements: Acknowledgements go to the contributing Organizations and also to the European Commission (EC)-supported *StandICT.eu* Project for supporting these industry activities aimed at progressing Standardization activities linked to 5G and its enablers—under sub-grantee contract number CALL04/20 (by Trust-IT Services Ltd, UK) for one of the contributing technical experts who is also Co-Editor of this paper (and is also contributing to the overall ETSI 5G PoC).

The ETSI 5G PoC Consortium as Whole:

Disclaimer: This White Paper expresses the opinion of the ETSI TC INT/AFI WG (formerly ETSI TCN NTECH AFI WG) 5G PoC Consortium Steering Committee and the other contributors.

"This AFI Proof of Concept has been developed according to the ETSI INT / ETSI NTECH AFI Proof of Concept Framework. AFI Proofs of Concept are intended to demonstrate AFI as a viable technology. Results are fed back to the Technical Committee on Network Technologies.

Neither ETSI, its Technical Committees INT and NTECH, nor their members make any endorsement of any product or implementation claiming to demonstrate or conform to AFI. No verification or test has been performed by ETSI on any part of this AFI Proof of Concept."