ETSI The Standards People

Generic Framework for E2E Federated GANA Knowledge Planes for AI-powered Closed-Loop Self-Adaptive Security Management & Control: Across Multiple 5G Network Slices, Segments, Services and Administrative Domains

TC INT/AFI GANA Framework: Autonomic Management and Control (AMC)

Presenters: **Dr. Ranganai Chaparadza (Capegemini/Vodafone consultant, Germany)**
Dr. Muslim Elkotob (Vodafone, Germany)
Dr. Tayeb Ben Meriem (Orange, France)
Dr. Benoit Radier (Orange, France)
Dr. Said Soulhi (Verizon, USA)

Welcome to the World of Standards

ETSI World Class Standards

GANA Distributed Autonomics Brain

orange™

TIM

Check Point SOFTWARE TECHNOLOGIES LTD

vodafone

ETSI AFI Proof of Concept

ALTRAN Part of Capgemini

IPv6 FORUM

Towards Standardization of 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

End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Networks

New Work Item Launched (Come Join!!):

https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63106

Contributors to the PoC Demo

- **Tayeb Ben Meriem, PhD: Orange:** Senior Standardization Manager & Technical Expert: ETSI TC-INT/AFI WG Chair; ETSI PoC Steering Committee Member; France
- **Ranganai Chaparadza, PhD: Altran CapGemini Germany:** Technical & Standardization Expert & Senior Consultant for Vodafone Consultant; IPv6 Forum; ETSI PoC Steering Committee Member; Germany
- **Muslim Elkotob, PhD: Vodafone:** Technical Expert and Solutions Design Architect & Standardization; Germany
- **Benoit Radier, PhD: Orange:** Standardization & Technical Expert; ETSI PoC Steering Committee Member; France
- **Eugen Hinz: Check Point Software Technologies GmbH**, Germany
- **Aviv Abramovich: Check Point Software Technologies**, Israel
- **Michael Stichel: Check Point Software Technologies GmbH**, Germany
- **Chris Federico: Check Point Software Technologies**, Israel, USA
- **Javier Padilla: Check Point Software Technologies**, Israel, USA
- **Ryan Darst: Check Point Software Technologies**, Israel, USA

Key Messages & Reflections on the Need for Autonomic (Closed-Loop) Security Management & Control in 5G, based on the White Paper No.6:

https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

AGENDA Outlook

- ETSI GANA Framework for Multi-Layer Autonomics, and the Integration of the ETSI GANA Knowledge Plane (KP) Platform Concept with SDN, NFV, Big-Data, OSS/BSS & Other Frameworks/Systems
- 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
- The Newly Launched Standardization Work Item on the Generic Framework in ETSI, and How to Join the Initiative and Contribute!
- Capabilities of Check Point Security Components & Functions that enable the Industry to Implement the Framework (in line with the ETSI GANA Framework)
- How Checkpoint Security Management Platform R80 can be used to implement GANA KPs' Security Management-DEs
- DEMO Carried Out on Autonomic Security Assurance for Differentiated Security SLAs for 5G Slices, while applying Security-as-a Service (SaaS) Model for Telcos

ETSI 5G PoC Consortium (Open)

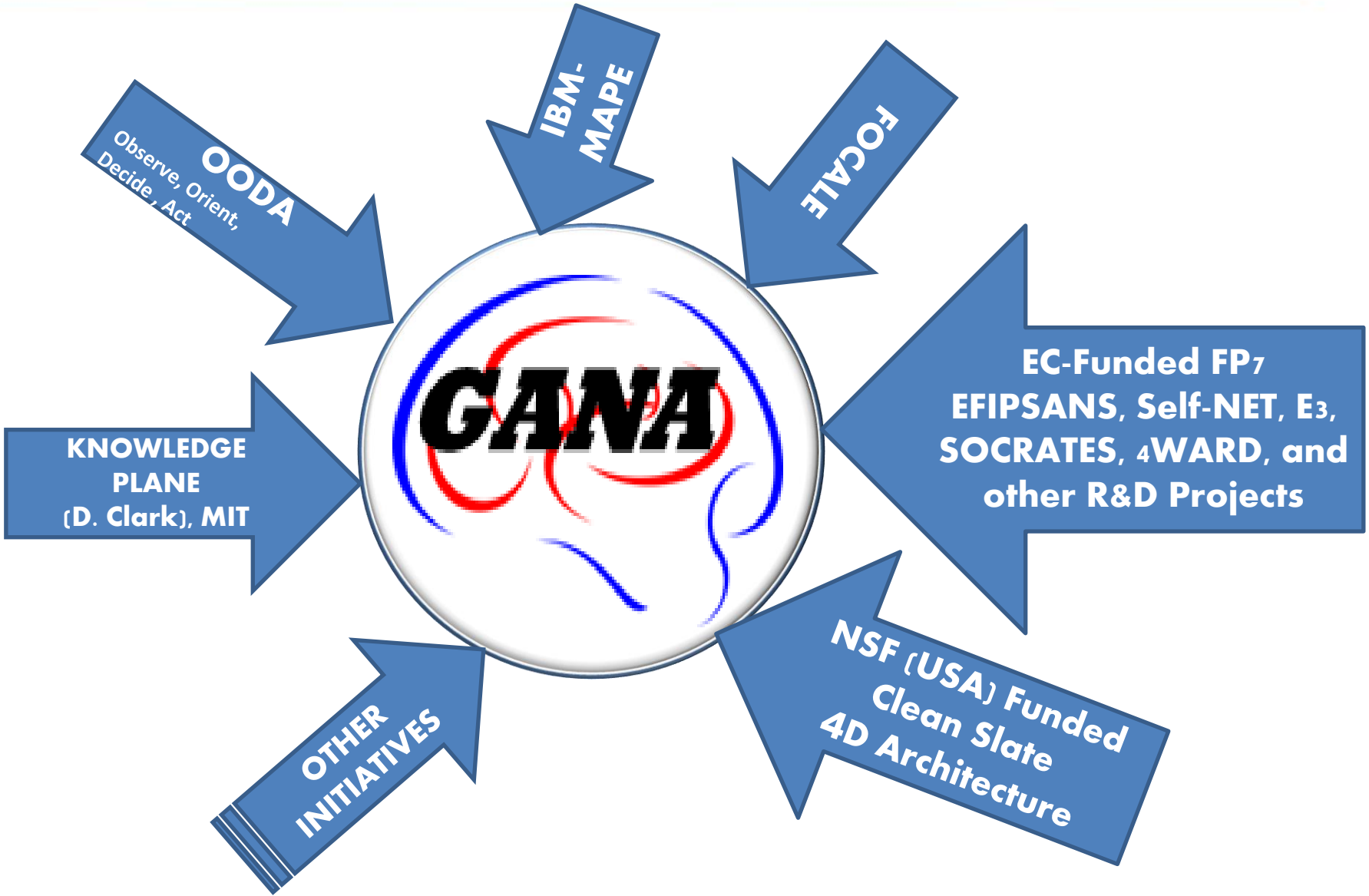
You are Invited to Join

- Orange
- Verizon
- NTT
- Telecom Italia
- Vodafone
- Altran
- Cellwize
- Huawei
- Incelligent
- QualyCloud
- IPv6 Forum
- Big Switch Networks
- Asocs Networks
- Softwell Performance AB
- Rohde & Schwarz
- DATAKOM
- Check Point

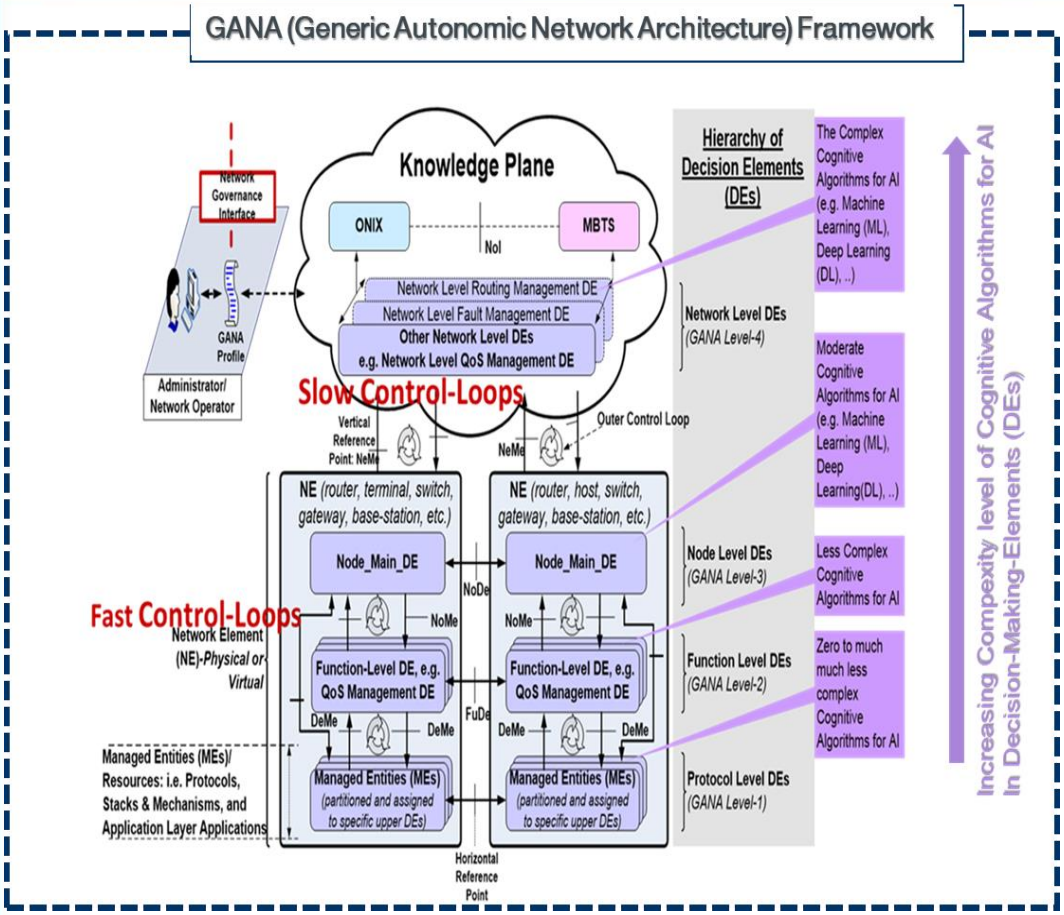
- Spirent
- Siemens
- Fraunhofer Fokus
- Ericsson
- Cinderella
- University of Göttingen

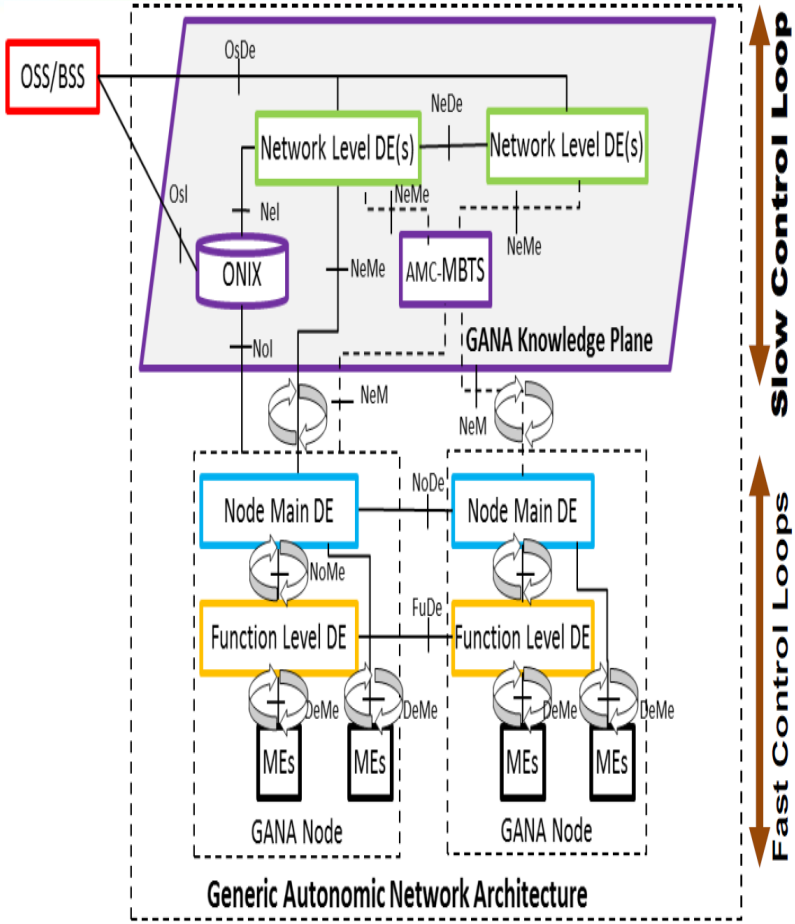
ETSI GANA Multi-Layer Autonomics and the Integration of the ETSI GANA Knowledge Plane (KP) with other systems, e.g. with Orchestrators, SDN Controllers, NFV MANO, and OSS/BSS or Configuration Management Systems

ETSI GANA as a Holistic & Unifying Model for AMC (Autonomic Management & Control) that fuses together the well-established models for AMC: (Reference : ETSI TS 103 195-2)



ETSI GANA (Generic Autonomic Networking Architecture) Reference Model / Functional Architecture (ETSI TS 103 195-2) for Multi-Layer AI & AMC





GANA is Framework for Multi-Layer Autonomic Management & Control (AMC)/Autonomics & Multi-Layer AI/ML for AMC

GANA Knowledge Plane (KP) Structure: Functional Blocks

Remark: ETSI White Paper No.16 and ETSI TS 103 195-2 describe the Recommendation to focus on GANA levels 2 to 4 when introducing autonomics in architectures and Why

ETSI TS 103 195-2 provides DE-to-its Managed Entities (MEs)

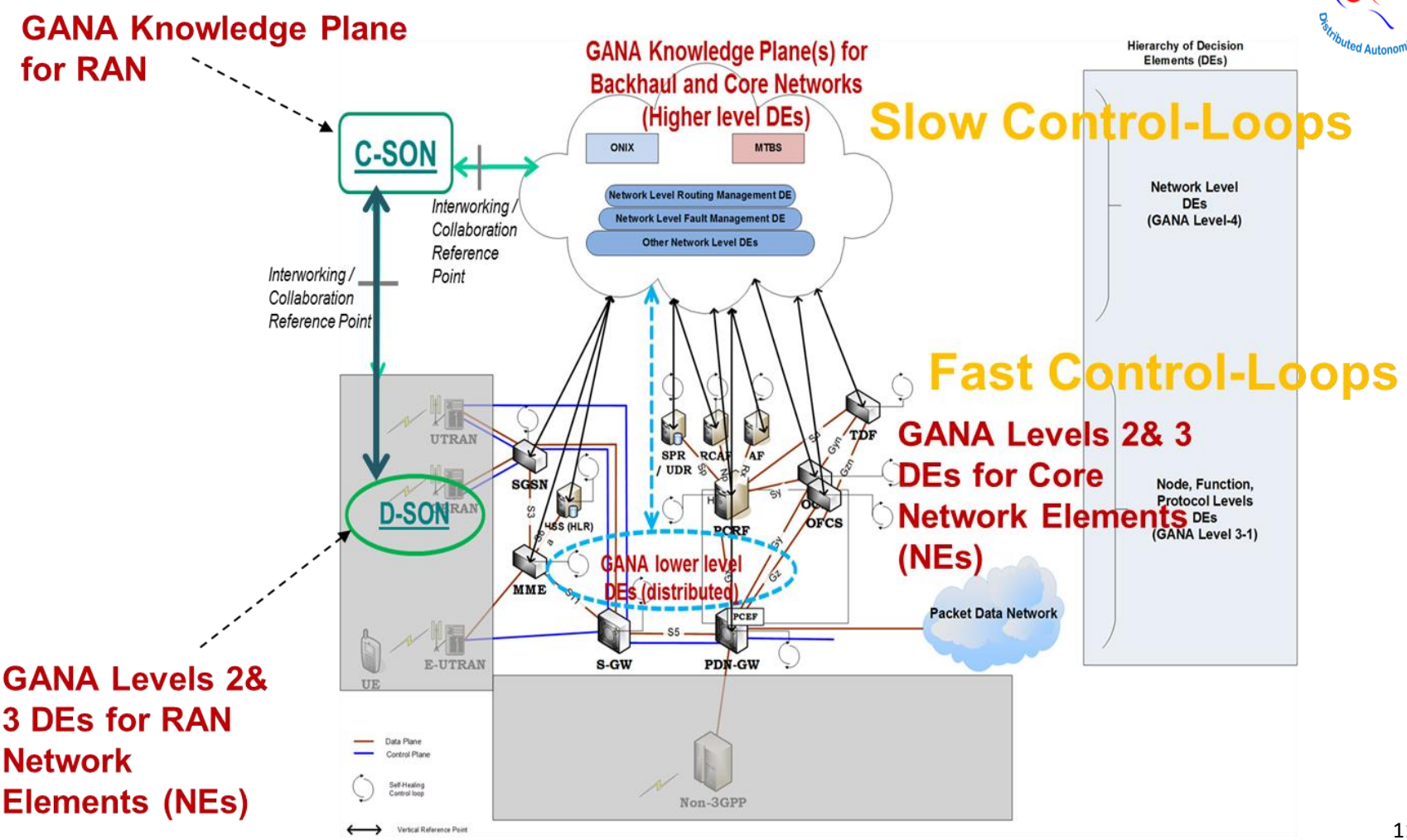
Mappings to Guide Implementations of DEs and Control-Loops

Network-Level DEs	Node-Level DEs	Function-Level DEs	Protocols and Mechanisms as Managed-Entities (MEs)	Examples of protocols and Mechanisms that are mapped as MEs
	GANA NODE			
NET_LEVEL_SEC_M_DE	NODE_LEVEL_SEC_M_DE		**Security Protocols, Algorithms and Mechanisms**	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, etc.
NET_LEVEL_FM_DE	NODE_LEVEL_FM_DE		Fault Detection Mechanisms, Fault Isolation/Localization/Diagnosis Mechanisms, Fault Removal Mechanisms	Active Probing mechanisms, Bi-Directional Forwarding Detection (BFD protocol) for link failure detection, Self-test/diagnose functions, rebooting, reloading, automated module replacement mechanisms, etc.
NET_LEVEL_RS_DE	NODE_LEVEL_RS_DE		Proactive and Reactive Resilience Mechanisms, Survivability Strategies and Algorithms, Restoration and Protection Mechanisms	Node Resilience mechanisms, and Network Resilience mechanisms, etc.
	NODE_LEVEL_AC_DE		Neighbour Discovery Protocols/Mechanisms and Network Discovery Mechanisms	Neighbour Discovery Protocol (NDP), Secure Neighbour Discovery Protocol (SEND), etc.
NET_LEVEL_RM_DE	NODE_MAIN_DE	FUNC_LEVEL_RM_DE	Routing Protocols and Mechanisms	OSPF, BGP, RIP, ISIS, etc.
NET_LEVEL_FWD_M_DE		FUNC_LEVEL_FWD_M_DE	Layer-3 Forwarding Protocols and Mechanisms, Layer-2.5-Fowarding, Layer-2-Fowarding, Layer-3-Switching, Layer-2-Switching, etc.	IPv4/IPv6 Forwarding Engine, Multi-Protocol Label Switching (MPLS), etc.
NET_LEVEL_QoS_M_DE		FUNC_LEVEL_QoS_M_DE	QoS Protocols and Mechanisms	Packet classifier, Packet Marker, Queue Management, Queue Scheduler, RSVP, etc.
NET_LEVEL_MOM_DE		FUNC_LEVEL_MOM_DE	Mobility Management Protocols and Mechanisms	Mobility Support in Internet Protocol Version 6 (MIPv6), Datagram Congestion Control Protocol, Mobile Stream Control Transmission Protocol, Site Multi-homing by IPv6 Intermediation, Proxy-Mobile-IP, Mobility-Management User-Equipment Managed-Entity, Measurement-Report-Function Managed-Entity, Candidate-Access-Router-Discovery mechanism, Fast Handover Scheme, Policy Control and Charging Rules Function mechanism, etc.
NET_LEVEL_MON_DE		FUNC_LEVEL_MON_DE	Monitoring Protocols, Mechanisms and Tools	IPFIX data collection and dissemination mechanisms, SNMP data collection and dissemination mechanisms, NETFLOW data collection and dissemination mechanisms, Protocol Analysers, Packet Trace creation and dissemination mechanisms. Effective and Available Bandwidth Estimation mechanisms, IPv6 hop-by-hop options for intrinsic monitoring, etc.
		FUNC_LEVEL_SM_DE	Services and Applications	Orchestration of services, service-discovery, interpretation of service and application requirements at run-time and requesting the network layer to behave in a service/application-aware manner, realizing a control-loop over the services/applications as its Managed Entities (MEs), collaboration with other DEs of responsible of autonomic management of the network layer protocols in order to realize collaborative self-adaptation on both the service-layer and the network-layer.

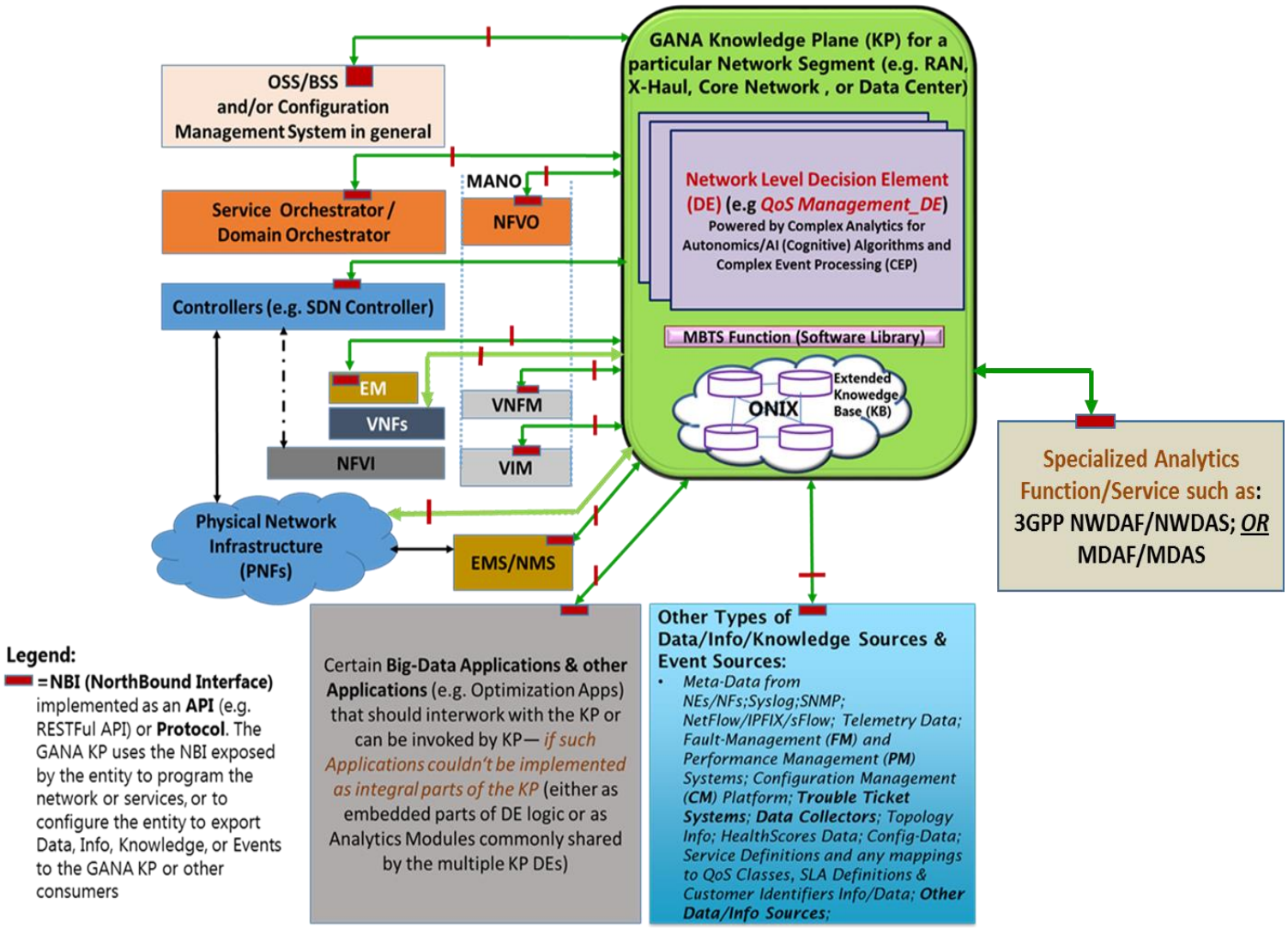
NOTE: There are other DEs that may have not been included in the Table 3 and implementers should take them into account based on their descriptions provided in the present document. Such DEs include Network-Level-Generalized Control Plane-Management-DE (NET-LEVEL-GCP_M_DE), Function-Level-Generalized Control Plane-Management-DE (FUNC-LEVEL-GCP_M_DE), Network Level End-to-End “end-user oriented” Service and Applications Management (NET_LEVEL_E2E_Service_M).

Example of a GANA Instantiation onto a particular Network Architecture and its associated Management & Control Architecture

Instantiation of GANA onto 3GPP EPC Core & Backhaul Network (ETSI TR 103 404); and Federated/Interworking GANA Knowledge Planes for RAN-, Backhaul- and 3GPP EPC Core Networks complemented by low level autonomics



GAN Multi-Layer Autonomics & AI and ETSI GANA Knowledge Plane(KP) Integration with other Systems



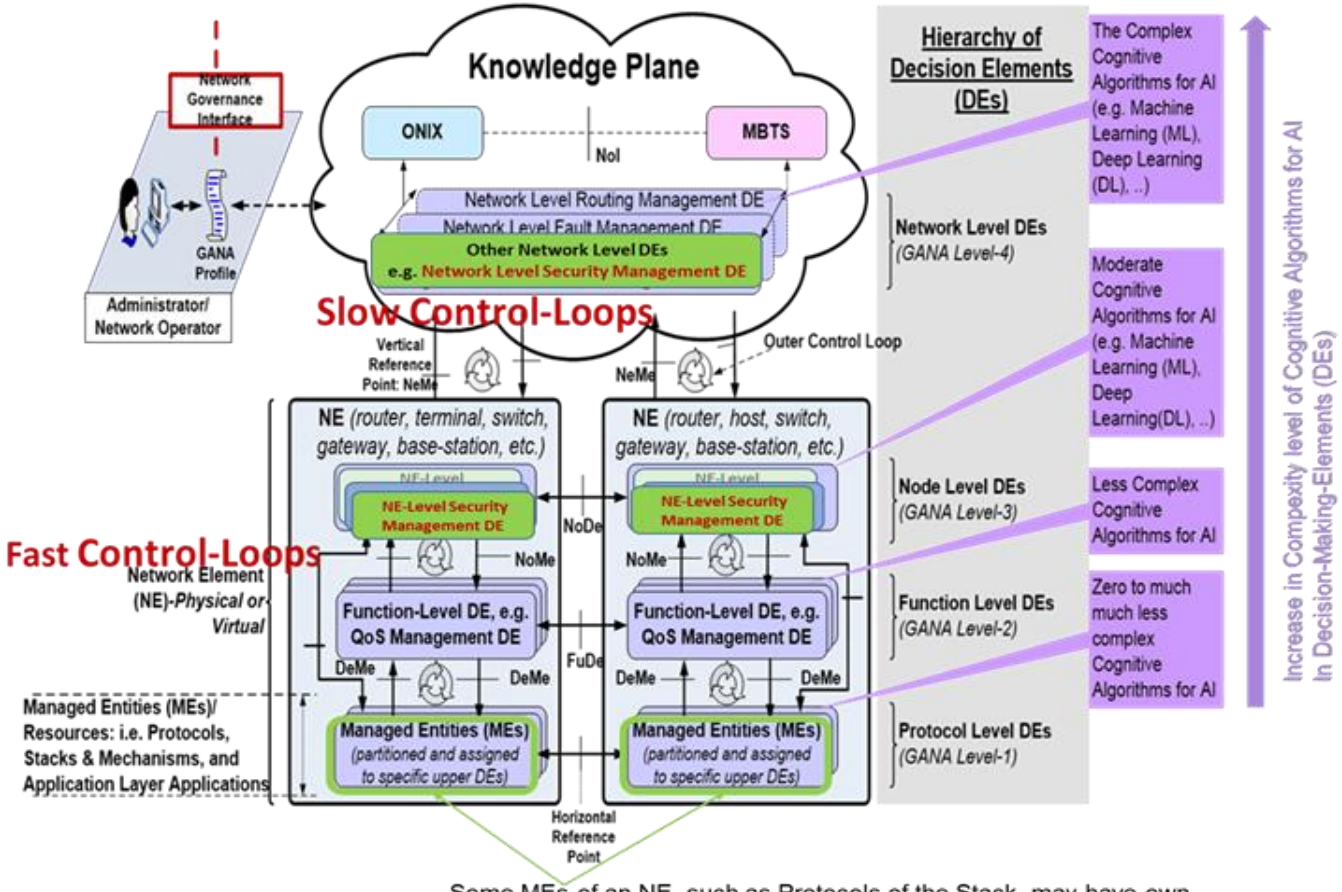
The Generic Framework for **Multi-Domain Federated ETSI GANA Knowledge Planes (KPs)** for End-to-End Autonomic (Closed-Loop) Security Management & Control **for 5G Slices, Networks/Services**

https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Autonomic Security Mgmnt & Control Architectures

ETSI TS 103 195-2

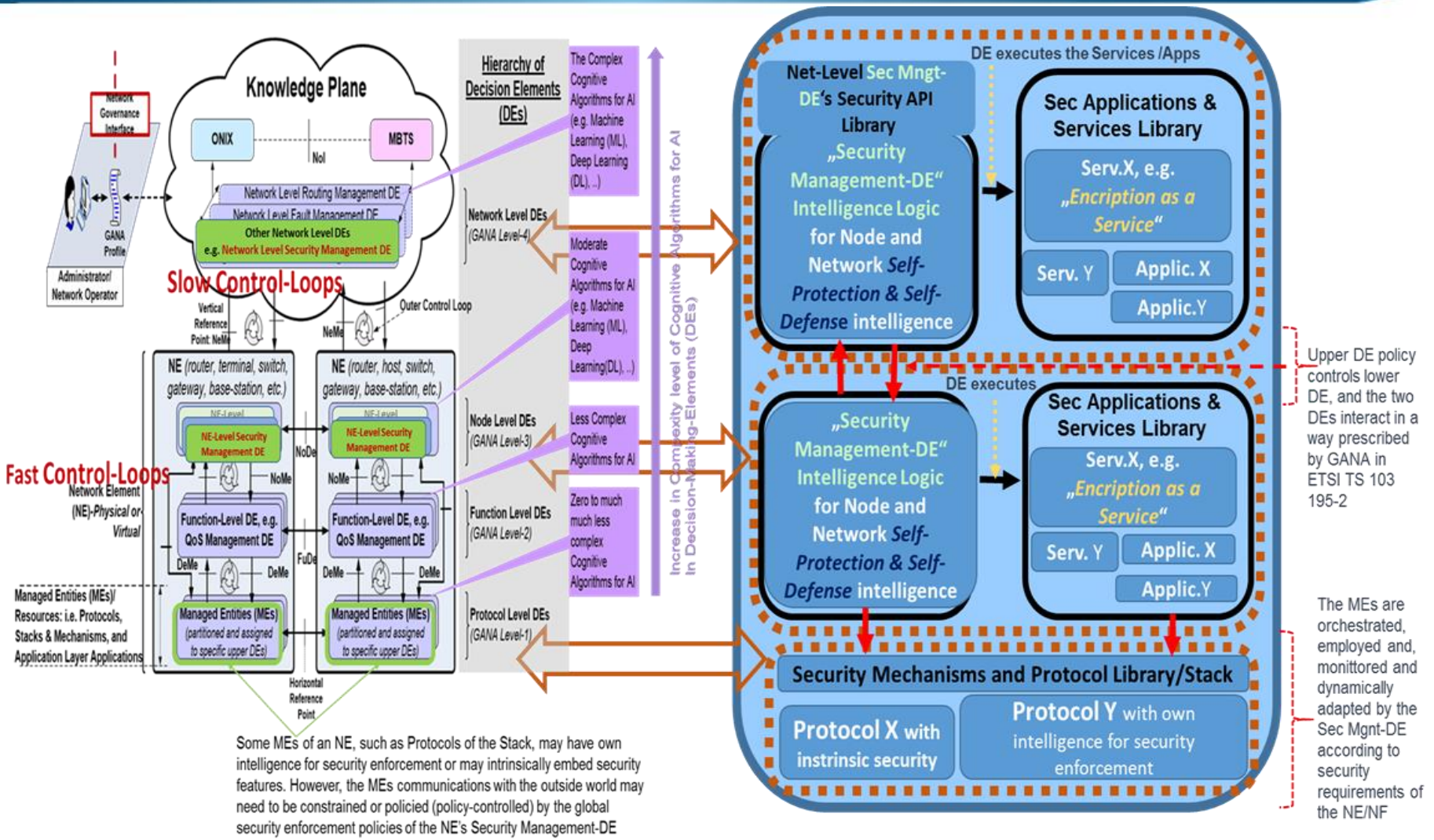
Instantiation onto CSPs' Networks (e.g. 5G Nets)



Some MEs of an NE, 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 policied (policy-controlled) by the global security enforcement policies of the NE's Security Management-DE

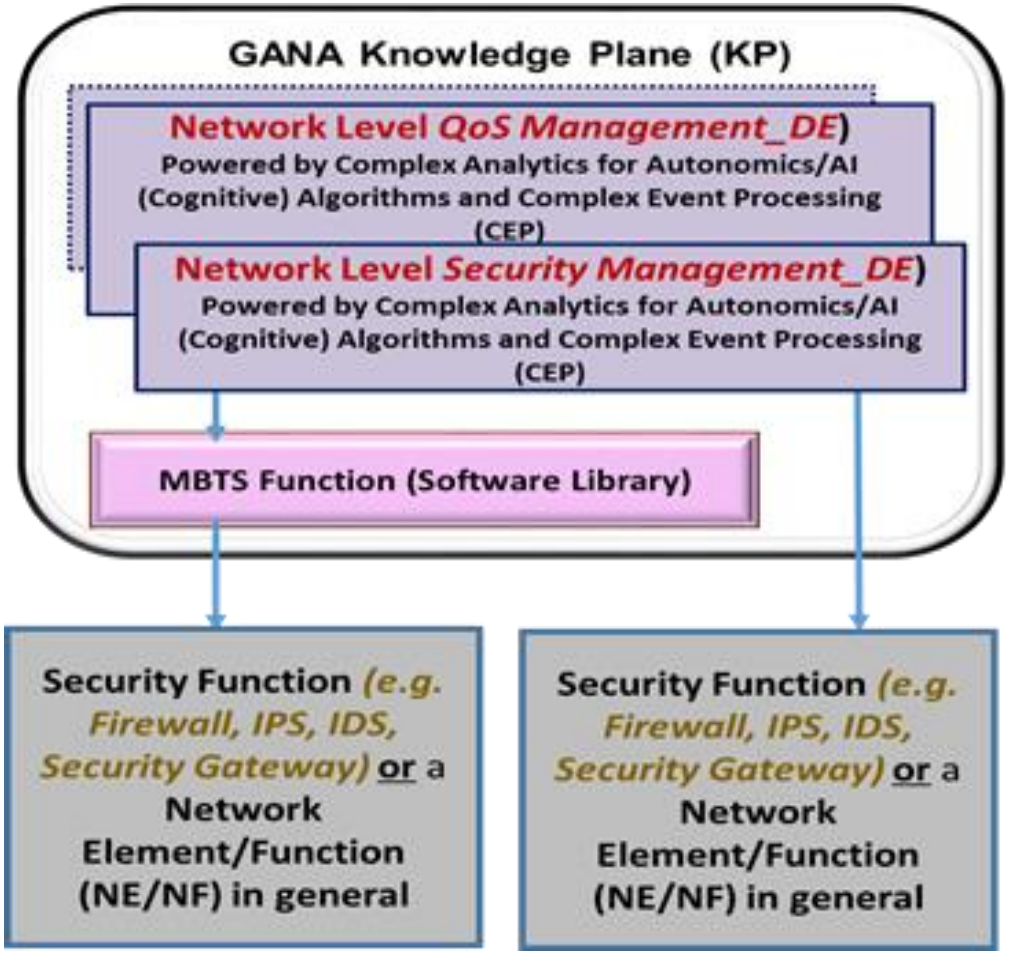
GANA is a Model for Multi-Layer Autonomics & Multi-Layer AI Models & Algorithms

Hierarchical Security Management & Control in GANA Framework and Security as a Service (SaaS) Enablers

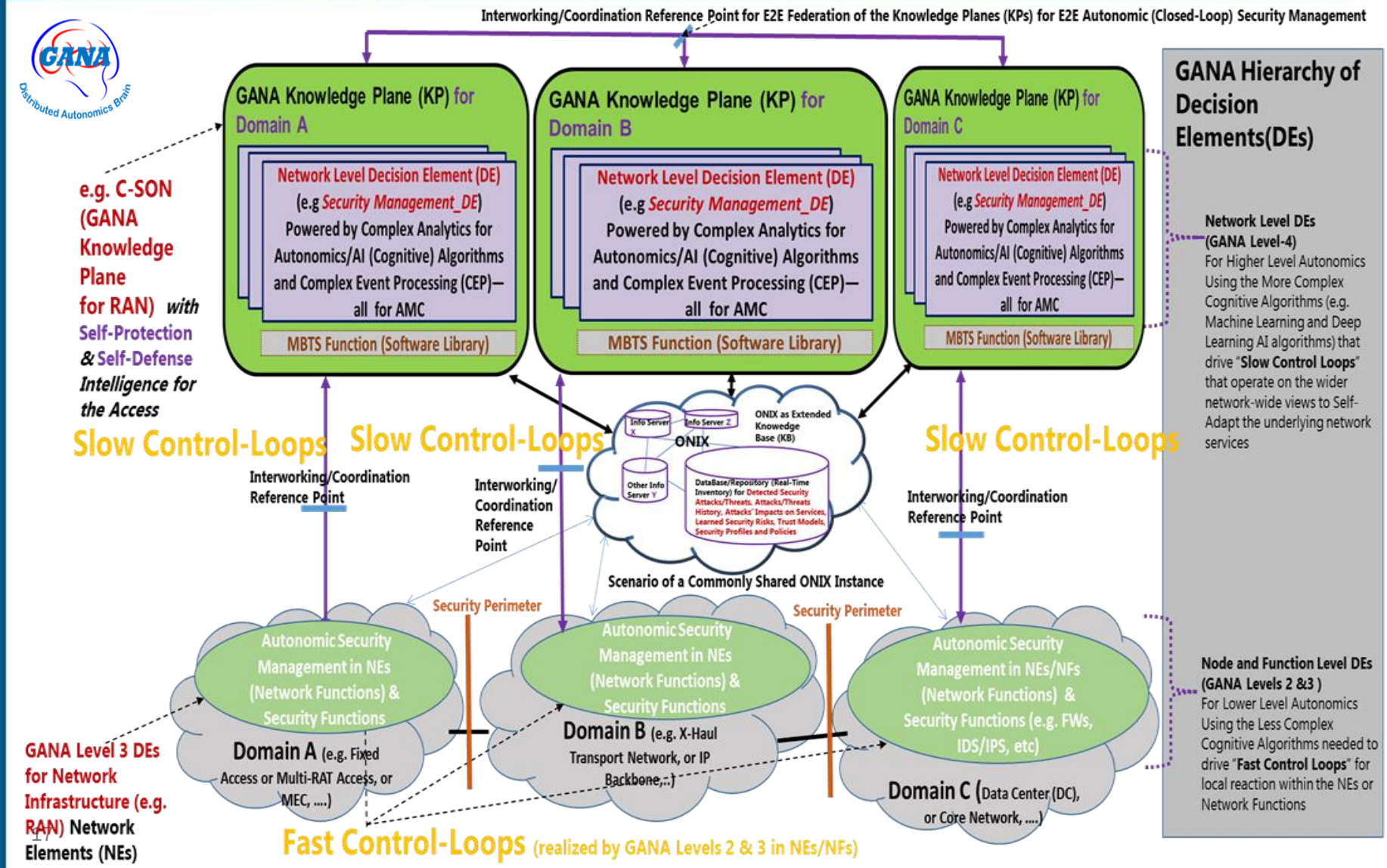


Some MEs of an NE, such as Protocols of the Stack, may have own intelligence for security enforcement or may intrinsically embed security features. However, the MEs communications with the outside world may need to be constrained or policied (policy-controlled) by the global security enforcement policies of the NE's Security Management-DE

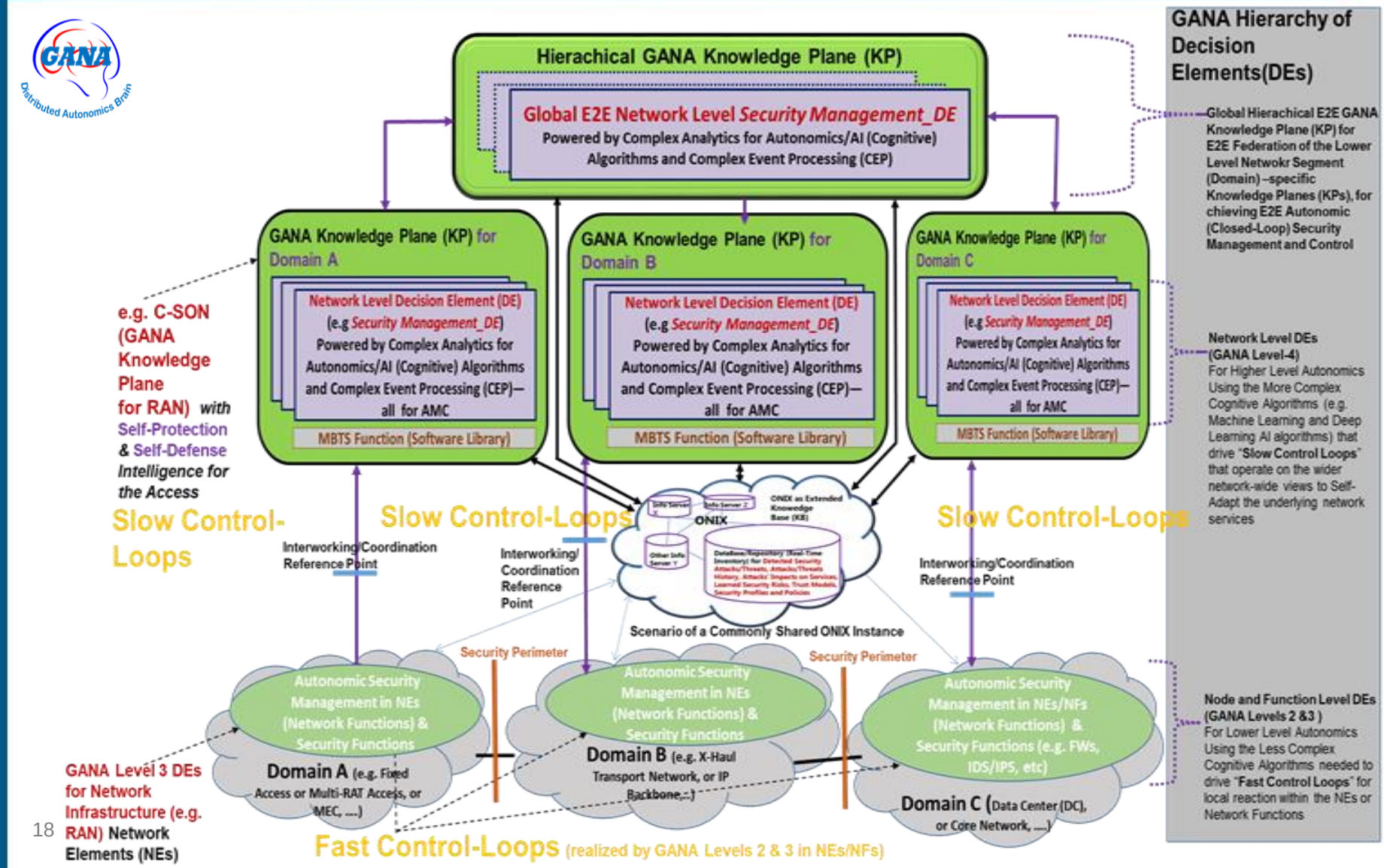
Security Management DE Programming Standalone Security Functions or Embedded in Network Functions



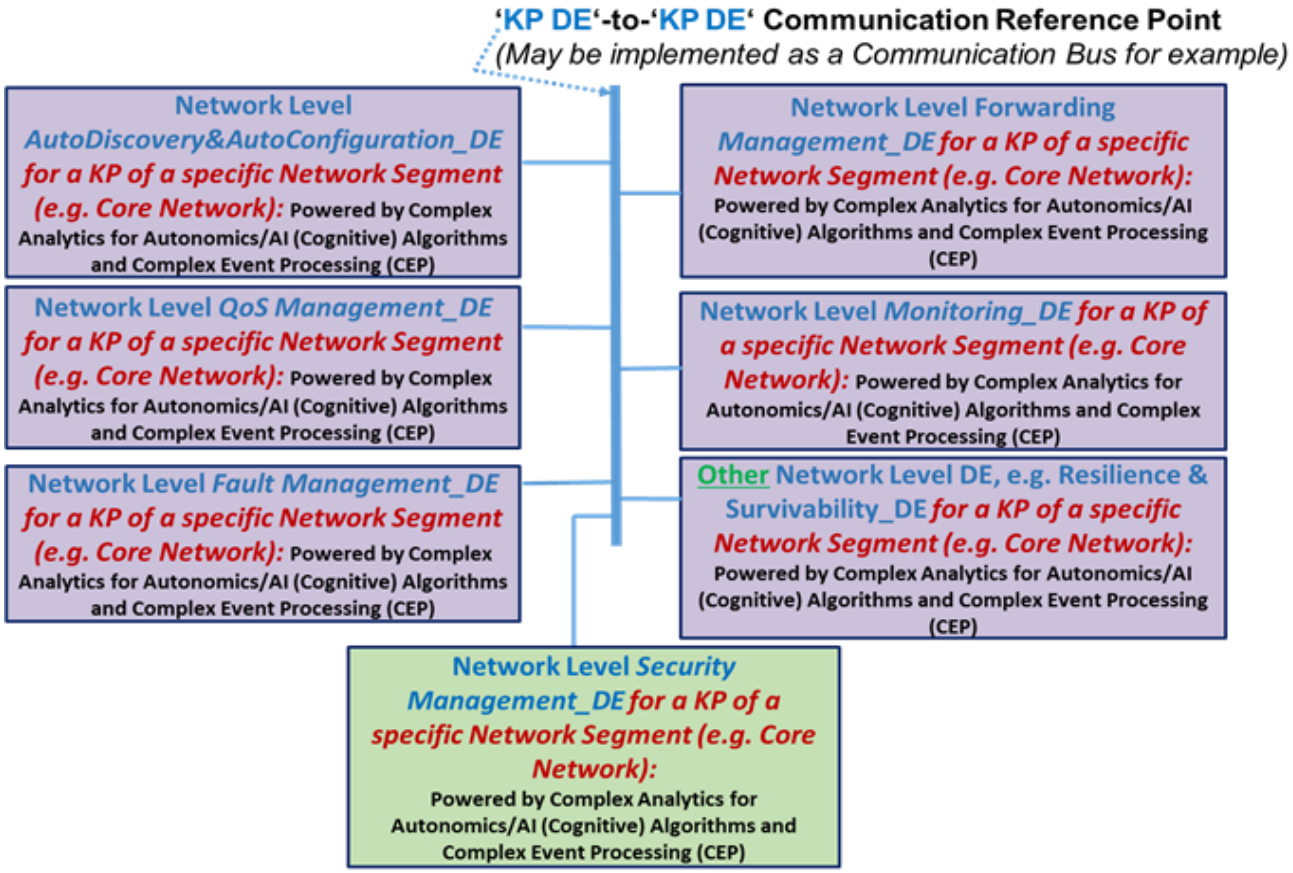
Federation of GANA KPs for E2E Autonomic Service & Security Assurance of 5G Slices :Horizontal Federation of KPs



Federation of GANA KPs for E2E Autonomic Service & Security Assurance of 5G Slices: Vertical/Hierarchical Federation of KPs



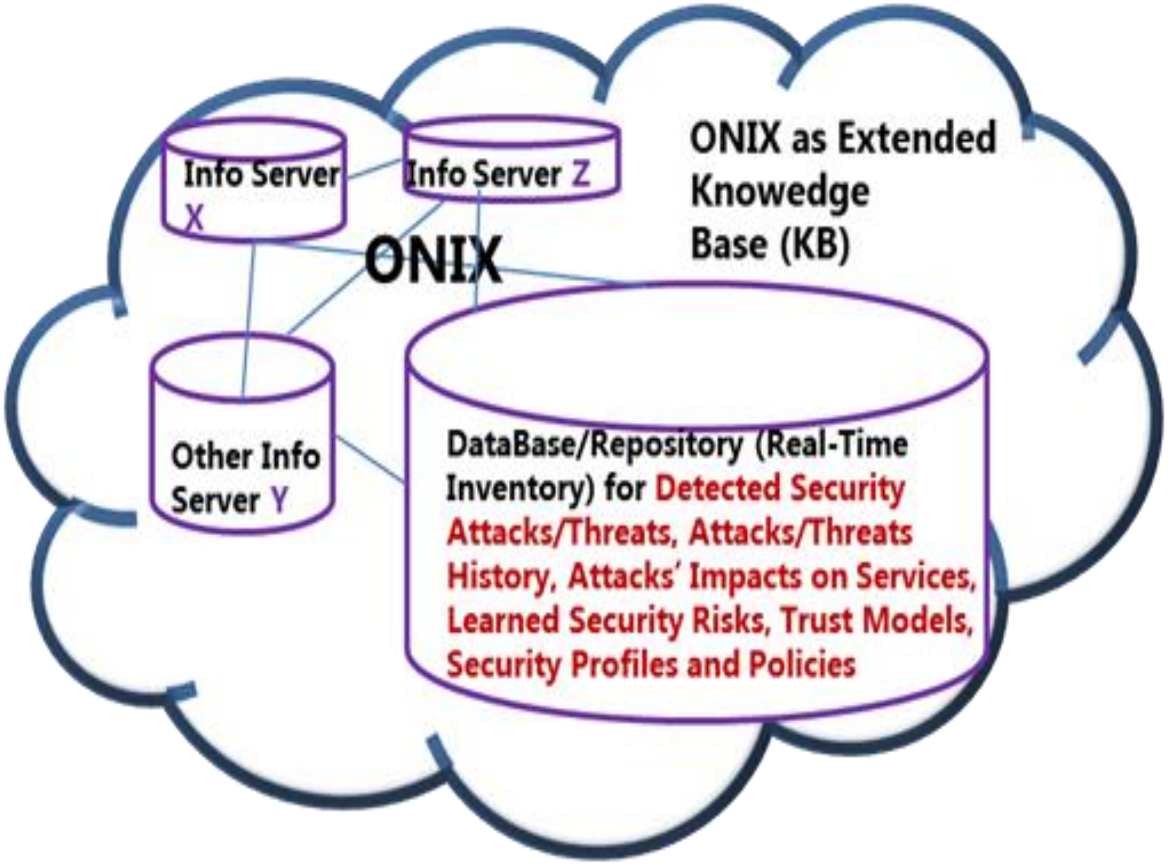
Intra-KP Decision Elements (DEs) Communications and Coordinations ; Implications on Self-Defense & Self-Protection



- *Self-Defence Strategies may require the Collaboration of the Security Management DE with 1 or More other DEs in attempts to Remediate against an Attack and eliminate the Negative Impact of the Attack*
- *Each KP DE should know the impact of the Attack to compute a Strategy on how its MEs could be orchestrated or re-configured to Minimize the Impact of the Attack, then Synchronize with the other KP DEs to find the best Converged Strategy Response to the Attack*

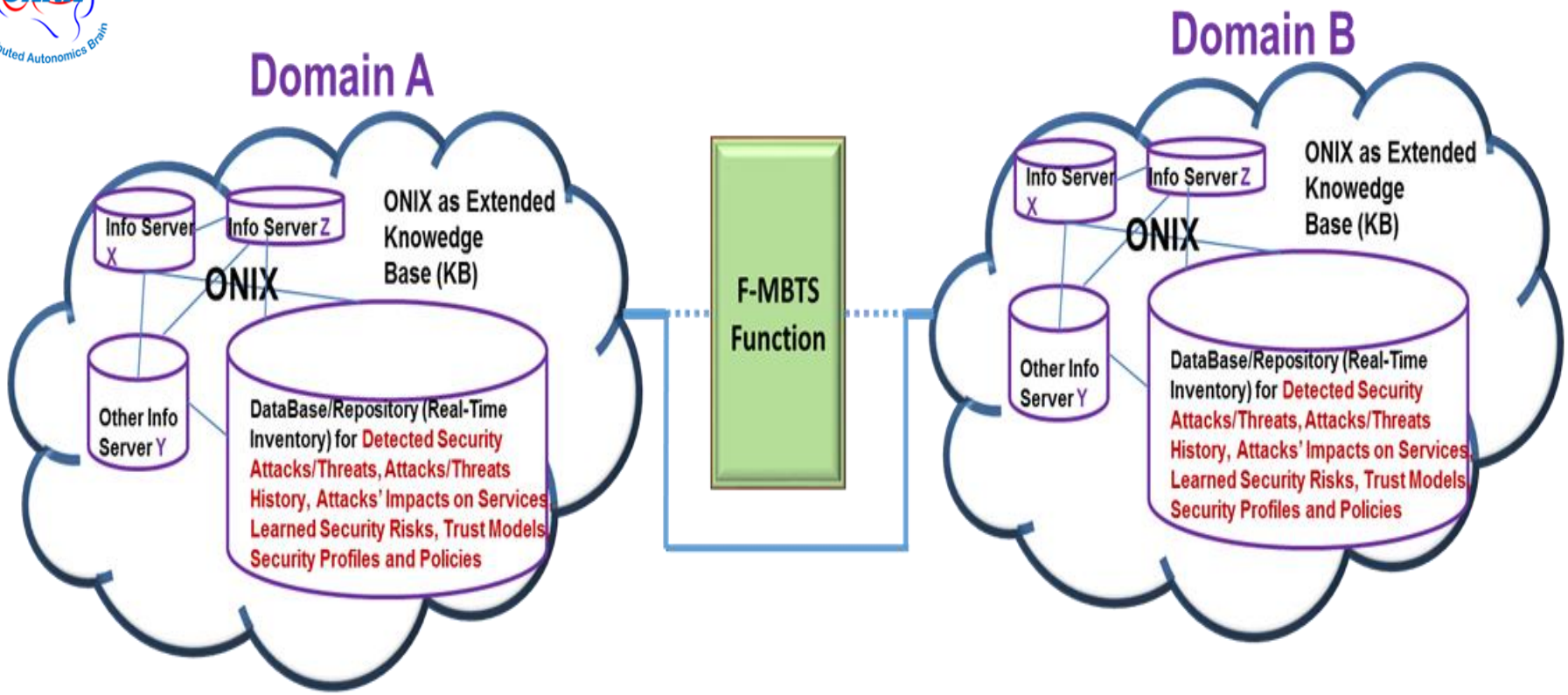
GANA ONIX – Real-Time Security Info/Knowledge Repository as part of ONIX Federated Information Servers

ONIX = *Overlay Network for Information Exchange*

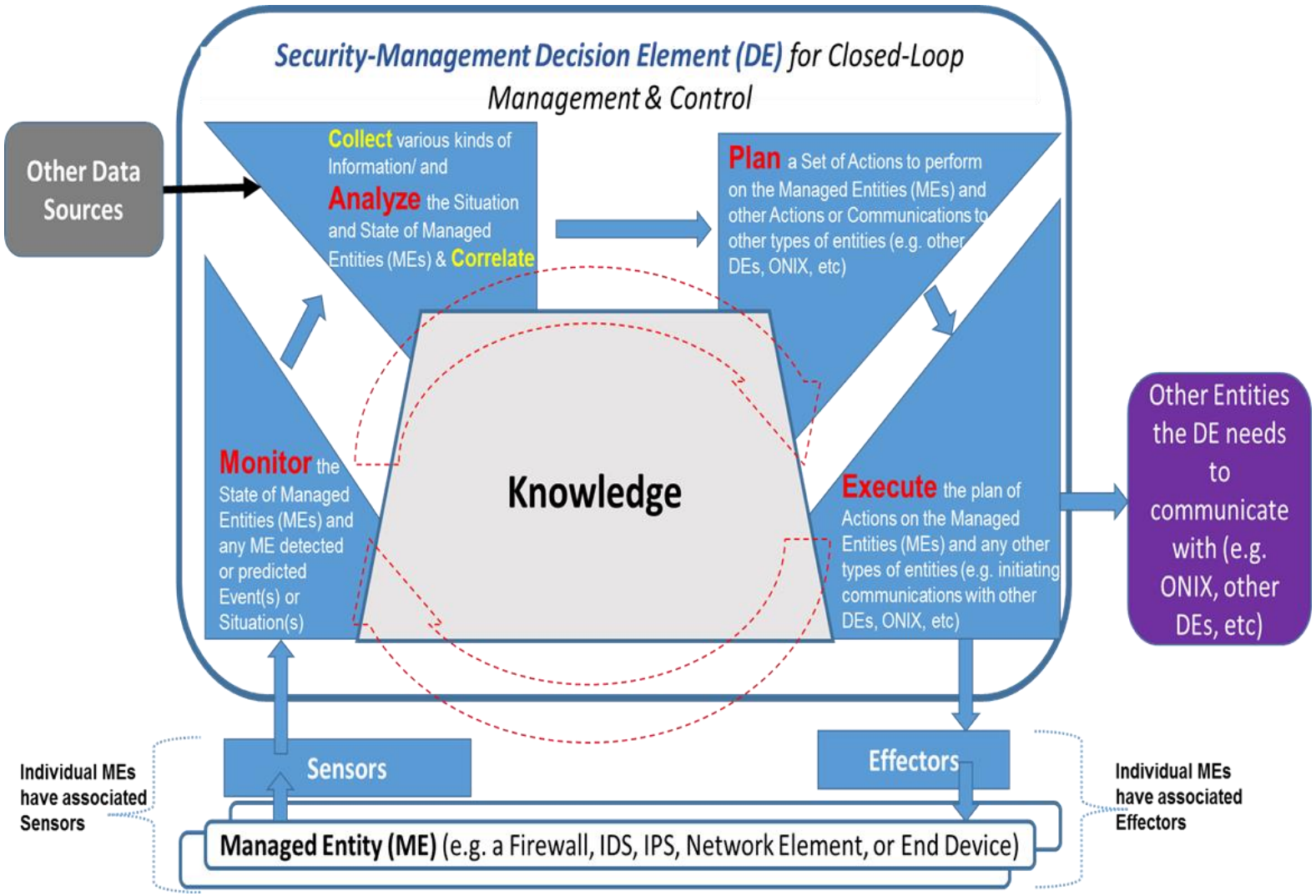


Federation of Real-Time Security Info/Knowledge Repositories Across Operators (as Multi-Domains)

ONIX = *Overlay Network for Information Exchange*



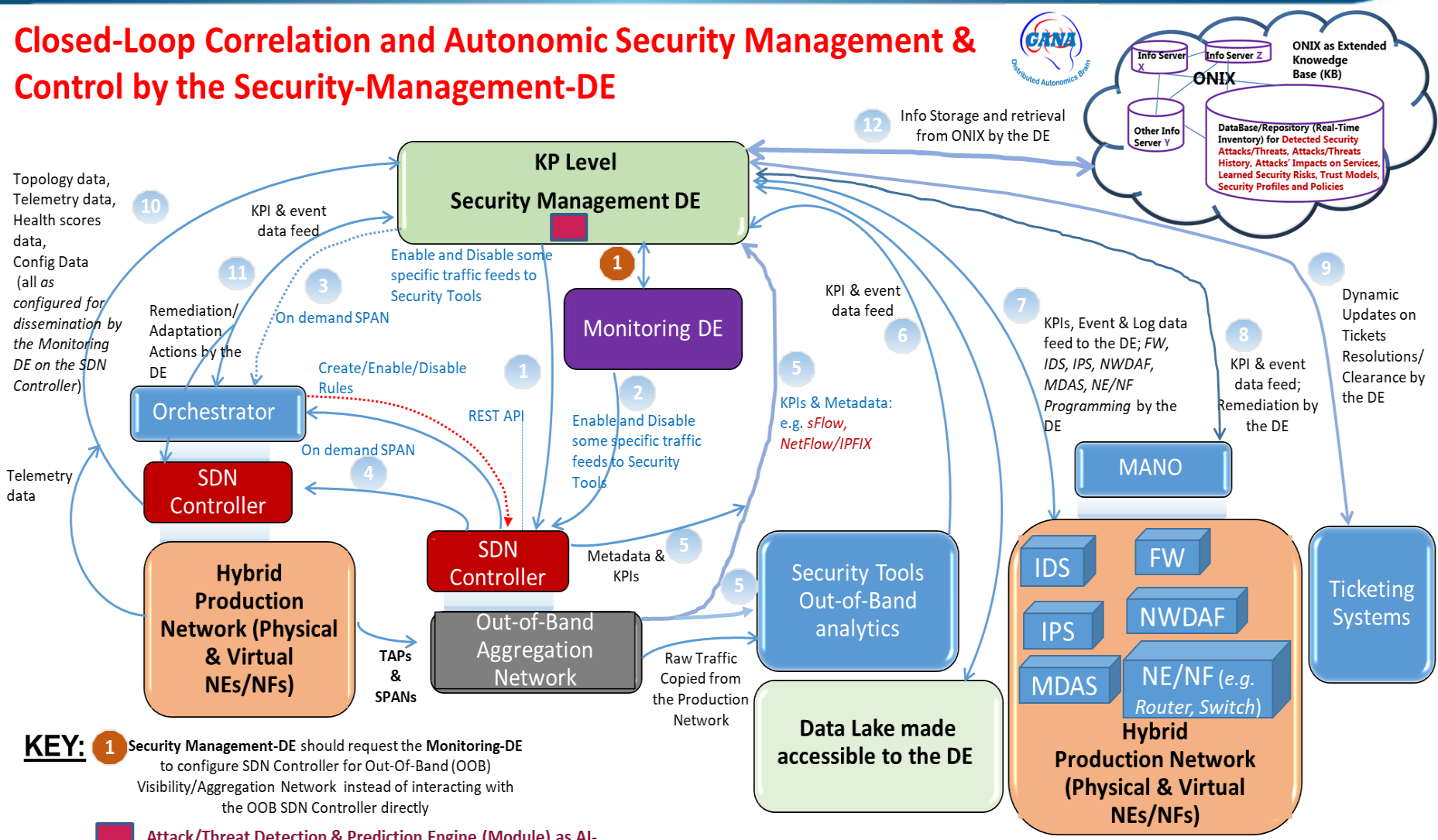
Example Approach on How to Design a GANA Decision Element (DE) Logic, e.g. based on IBM MAPE-K Model



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Correlation Role of a Security-DE in Open / Closed-Loop Autonomic Security Management & Control

Closed-Loop Correlation and Autonomic Security Management & Control by the Security-Management-DE



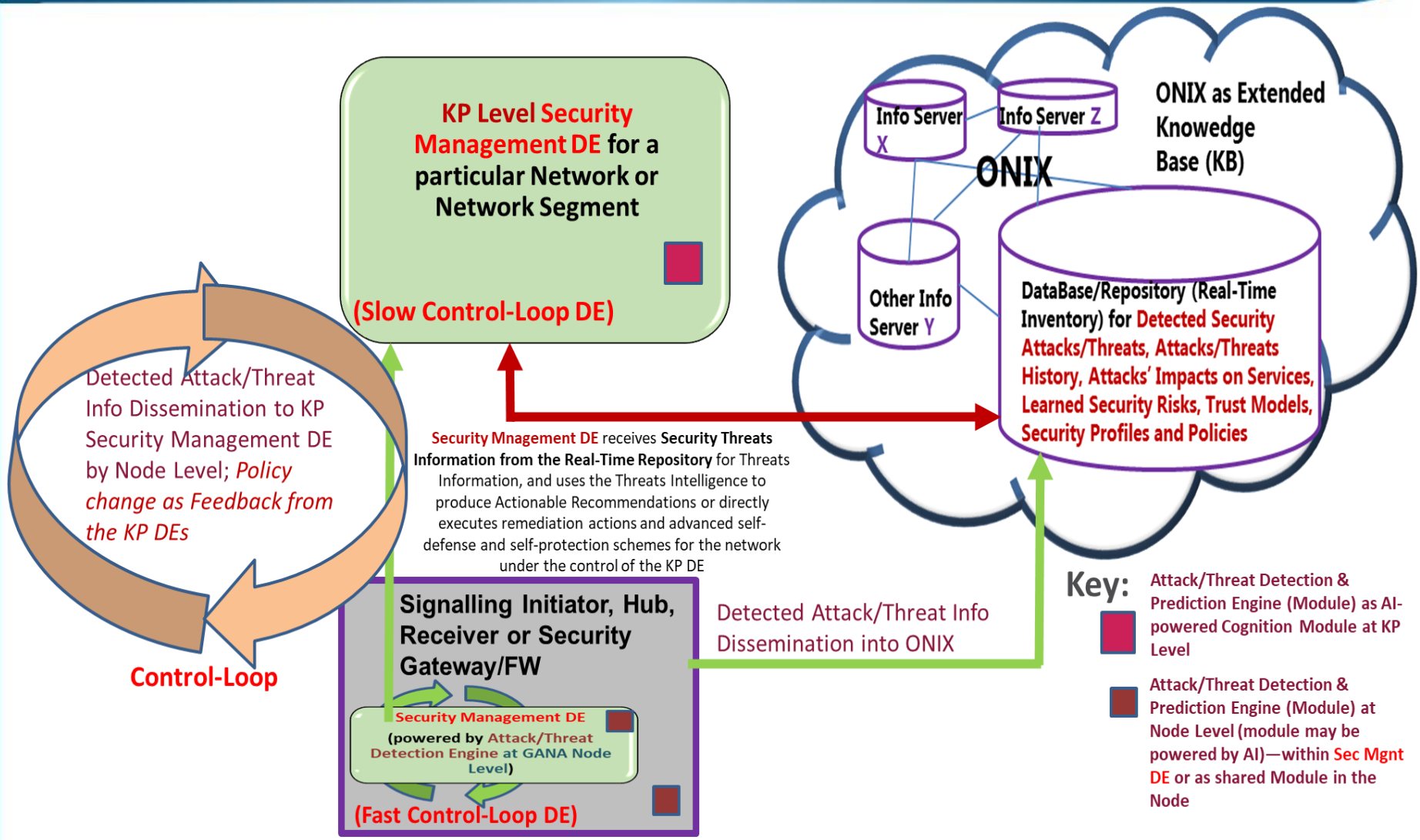
KEY: 1 **Security Management-DE** should request the **Monitoring-DE** to configure SDN Controller for Out-Of-Band (OOB) Visibility/Aggregation Network instead of interacting with the OOB SDN Controller directly

Attack/Threat Detection & Prediction Engine (Module) as AI-powered Cognition Module at KP Level

https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Illustration of the 2-Levels Security Mgnt DEs Coordination:

Self-Protection and Self-Defense Against Detected and Predicted Attacks on Signalling Protocols



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

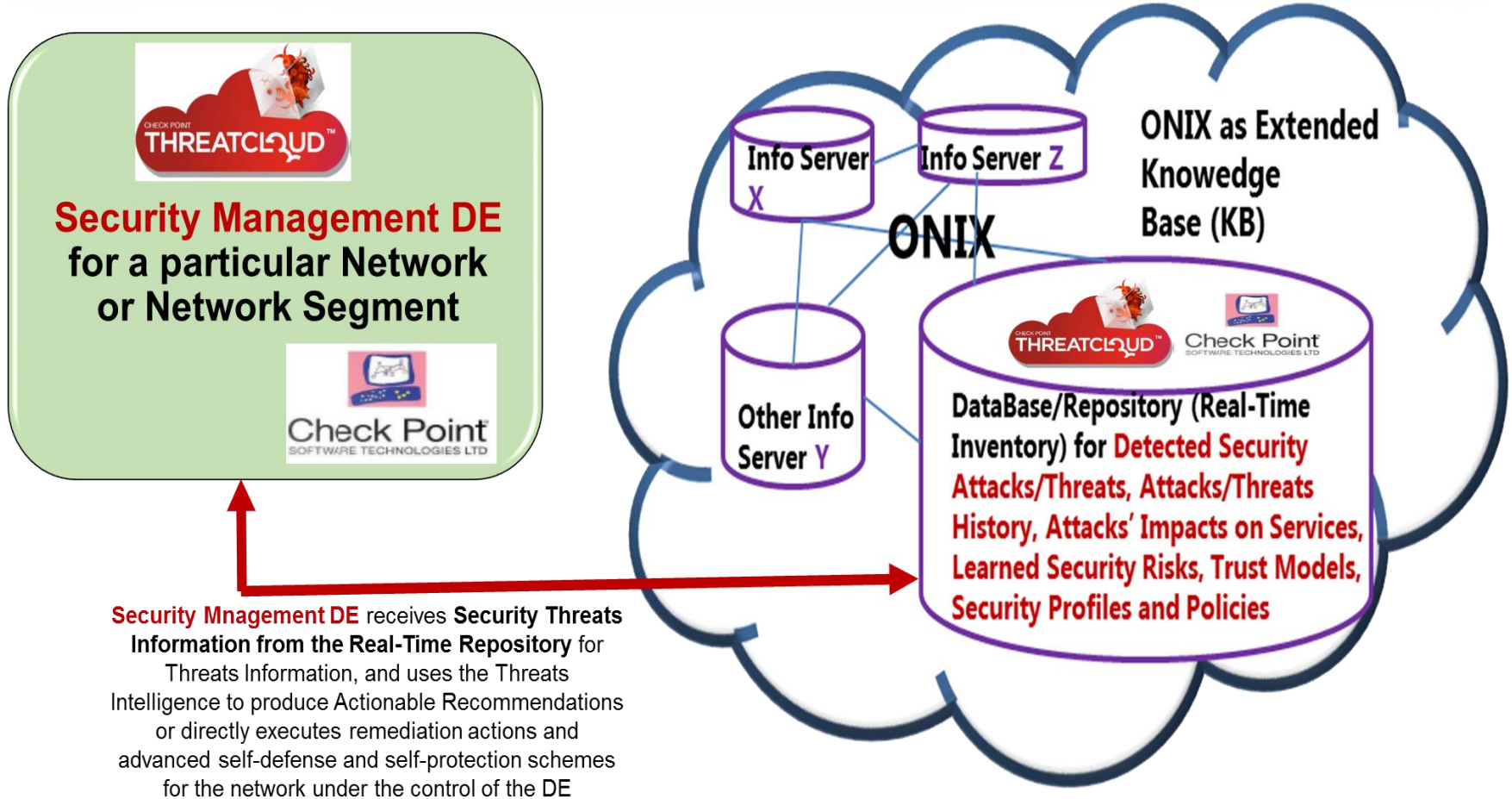
You are Invited to Contribute to the New Work Item that has been Launched in ETSI on the Standardization of the Framework !!

- This Presentation offered the opportunity to raise awareness of the fact that ETSI TC INT AFI WG is has now Laucnhed a New Standardization **Work Item** on **Generic Framework for Multi-Domain (Cross-Domain) E2E Federated ETSI GANA Knowledge Planes (KPs) Platforms for E2E Autonomic (Closed-Loop) Security Management & Control for 5G Slices, Network Segments and Services across Multiple Network and Administrative Domains of the E2E 5G Network Architecture**, to now commence the standardization of the Framework due to the very successful ETSI 5G PoC Results on this topic
- **Readers are encouraged to Join the Newly Launched Work Item in ETSI and Contribute:**
  https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63106

Capabilities of Check Point Security Components & Functions that enable the Industry to Implement the Framework *(in line with the ETSI GANA Framework)*

https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Implementation of Security Management-DE and Real-Time Repository for Threats Information using the CheckPoint Threat Cloud

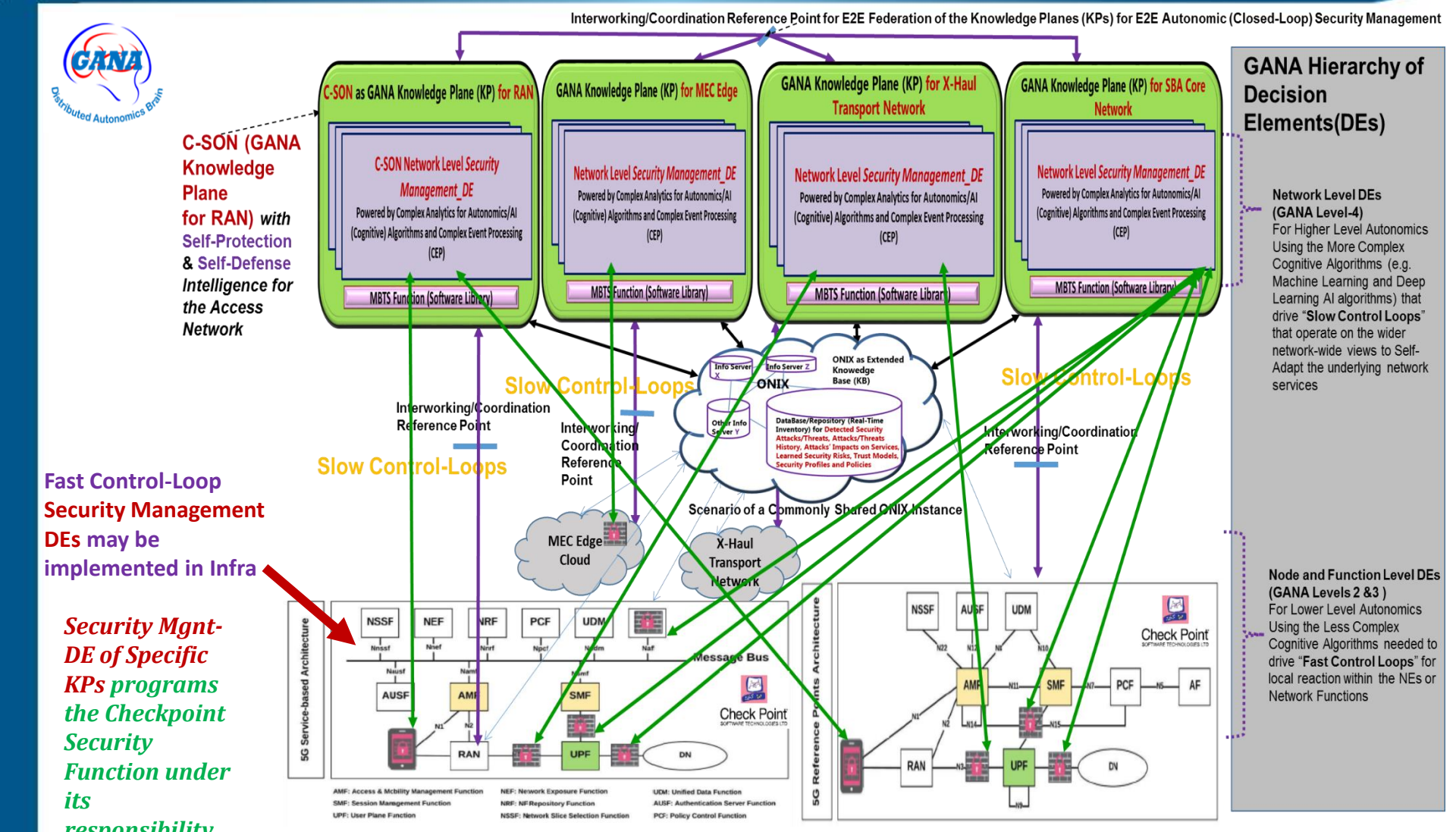


Security Mnagement DE receives **Security Threats Information from the Real-Time Repository** for Threats Information, and uses the Threats Intelligence to produce Actionable Recommendations or directly executes remediation actions and advanced self-defense and self-protection schemes for the network under the control of the DE

Currently the Security-Management-DE is implemented in the ThreatCloud to run in Open-Loop Mode but can be made to run in Closed-Loop Mode.

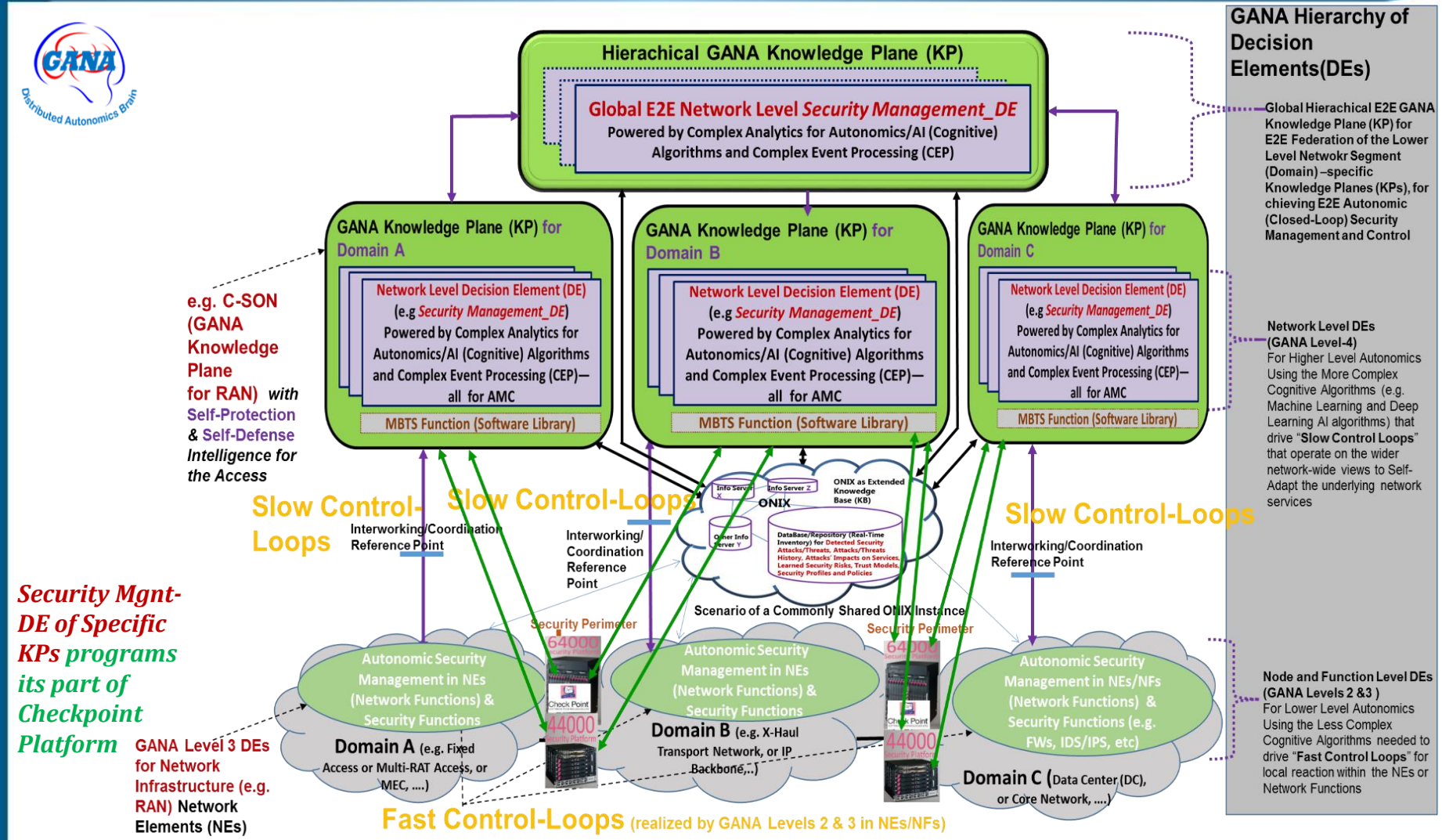
https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Check Point Programmability: Option-A: Horizontal Federation of GANA Knowledge Plane (KP) Platforms, and



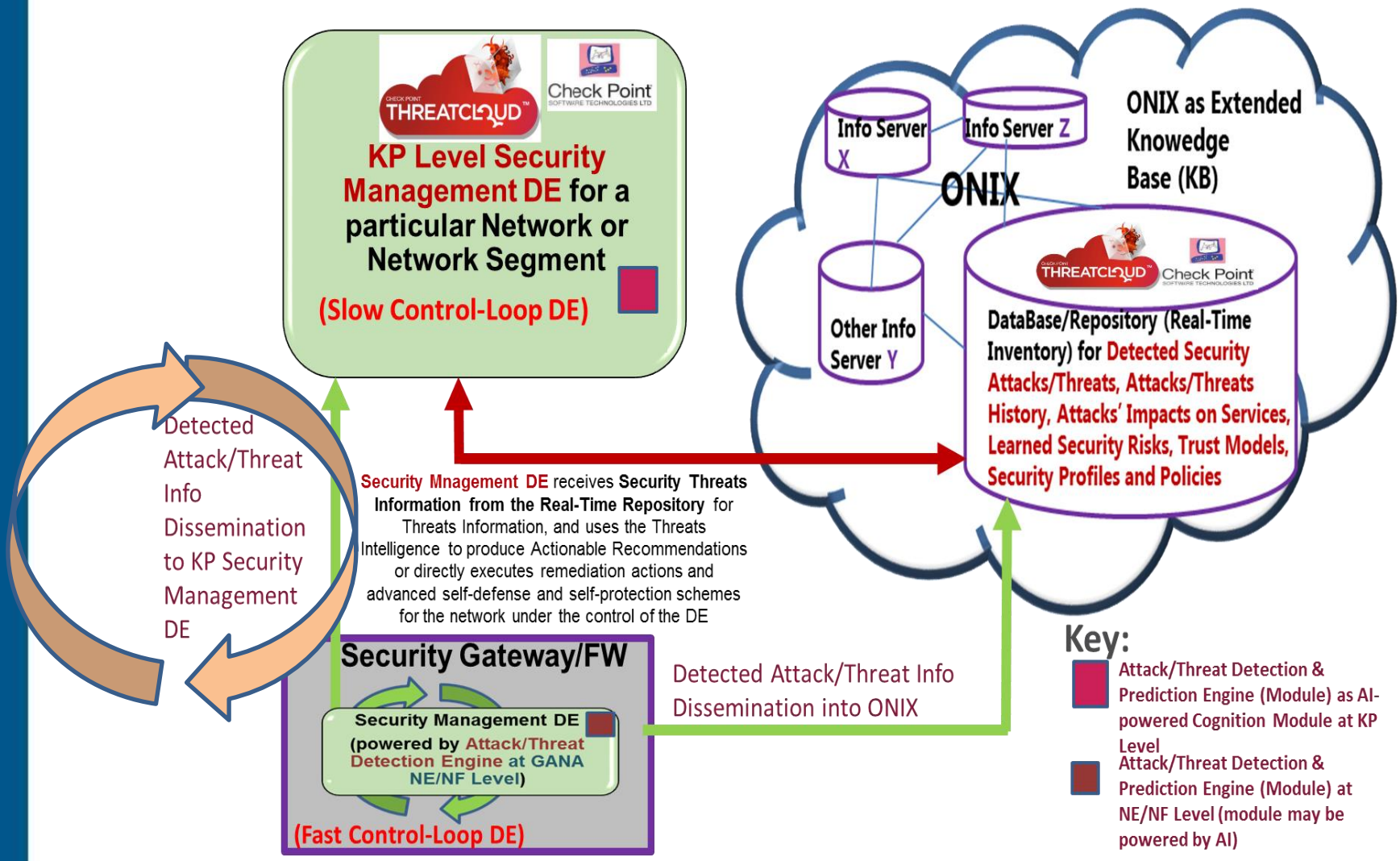
https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Check Point Programmability: Option-B: Hierarchical Federation of GANA Knowledge Plane (KP) Platforms,



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

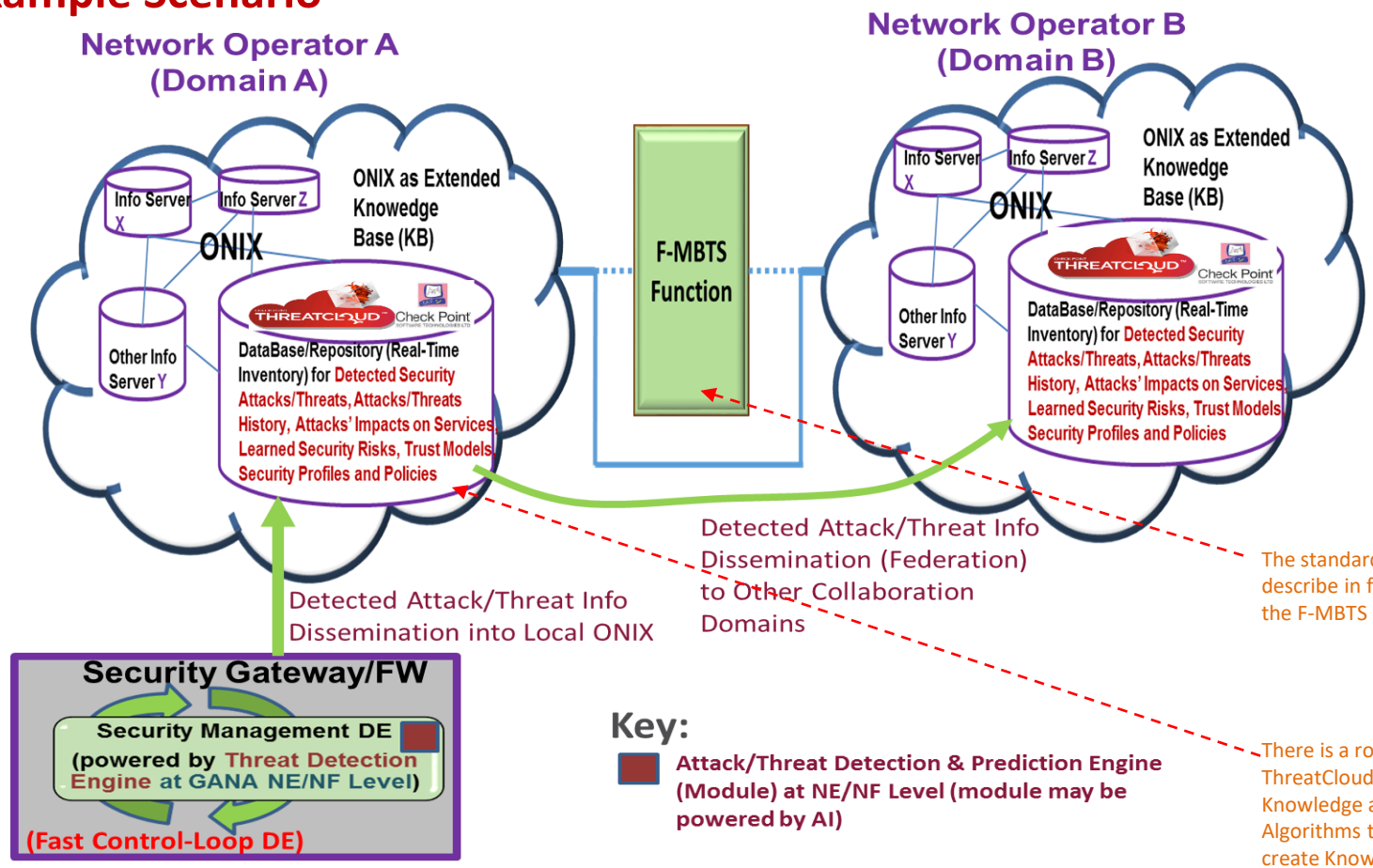
Interworking of the GANA KP Level Security Management DE and NE/NF Level Security Management DE and ONIX



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Detected Attack/Threat Info Dissemination (Federation) within the Same Operator Domain & to Other Collaboration Operator Domains

Example Scenario



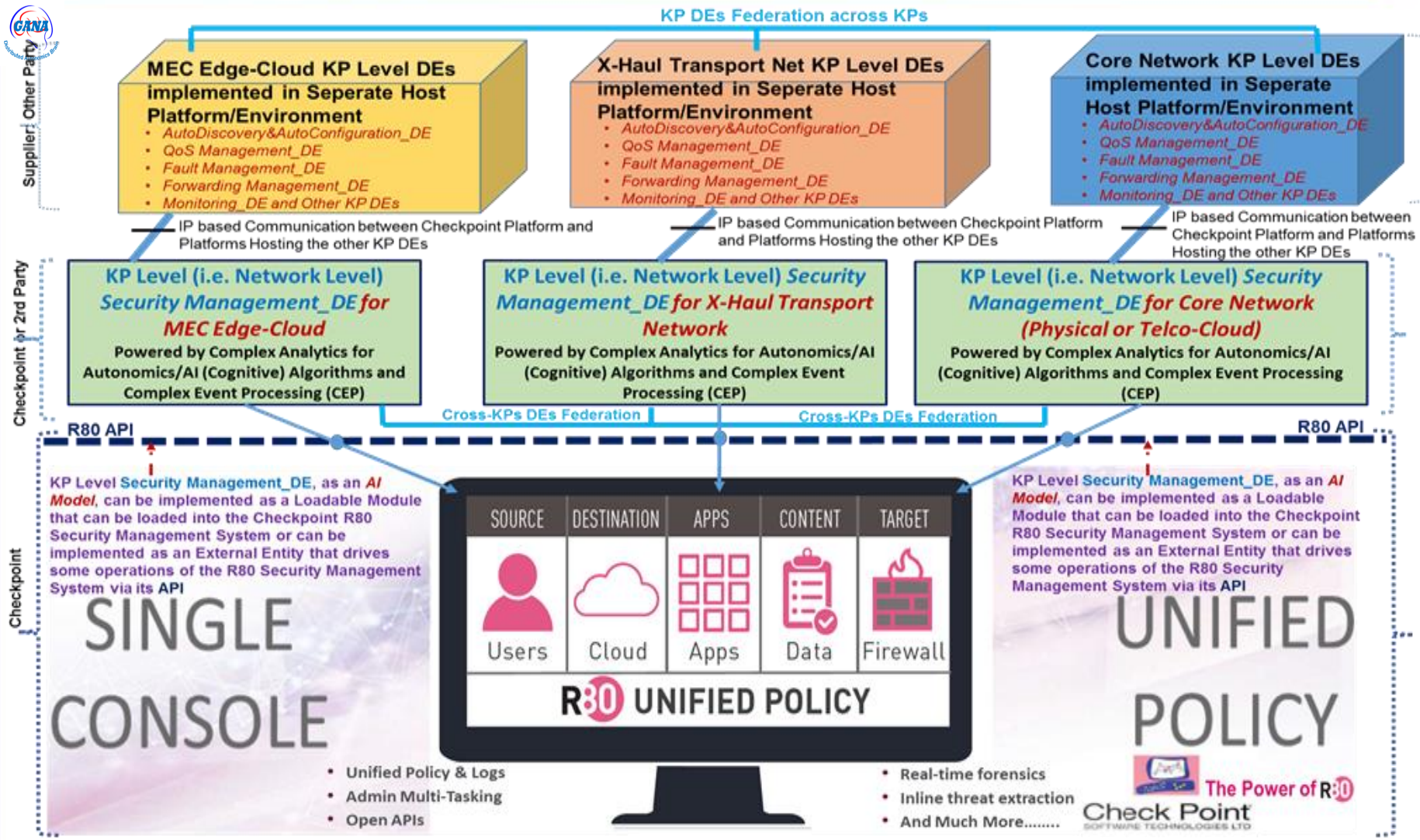
CheckPoint ThreatCloud Capability for Implementing the Realtime Inventory for Security Info/Knowledge can be used for Federation of the Info/Knowledge across Multiple Operators and Multi-Domains https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Check Point Security Management Platform R80 can be used to implement GANA KPs' Security Management-DEs

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

The R80 Management API of the Checkpoint Security Management R80 Platform can be used in enhancing it with GANA Security Management-DEs(characterized as AI Models that customize the operations of the Checkpoint Security Management R80 Platform)

Using the Check Point Platform R80 to implement Security Management-DEs of KPs for specific Network Segments



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Demo Part: Autonomic Security Assurance for Differentiated Security SLAs for 5G Slices, while applying Security-as-a Service (SaaS) Model for Telcos

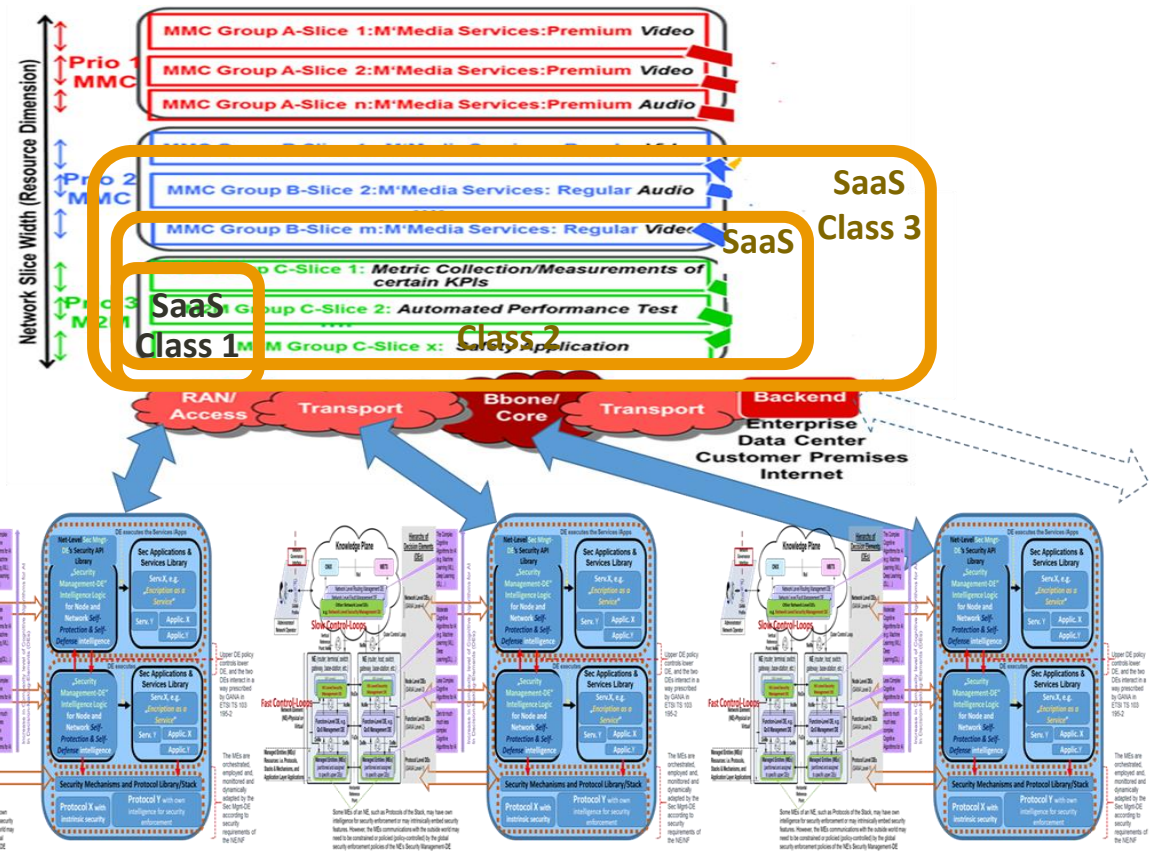
SaaS Vertical Segmentation

Vertical SaaS Segmentation (Across all tiers MEC through Core):

Class 1 SaaS: DDoS protection UE

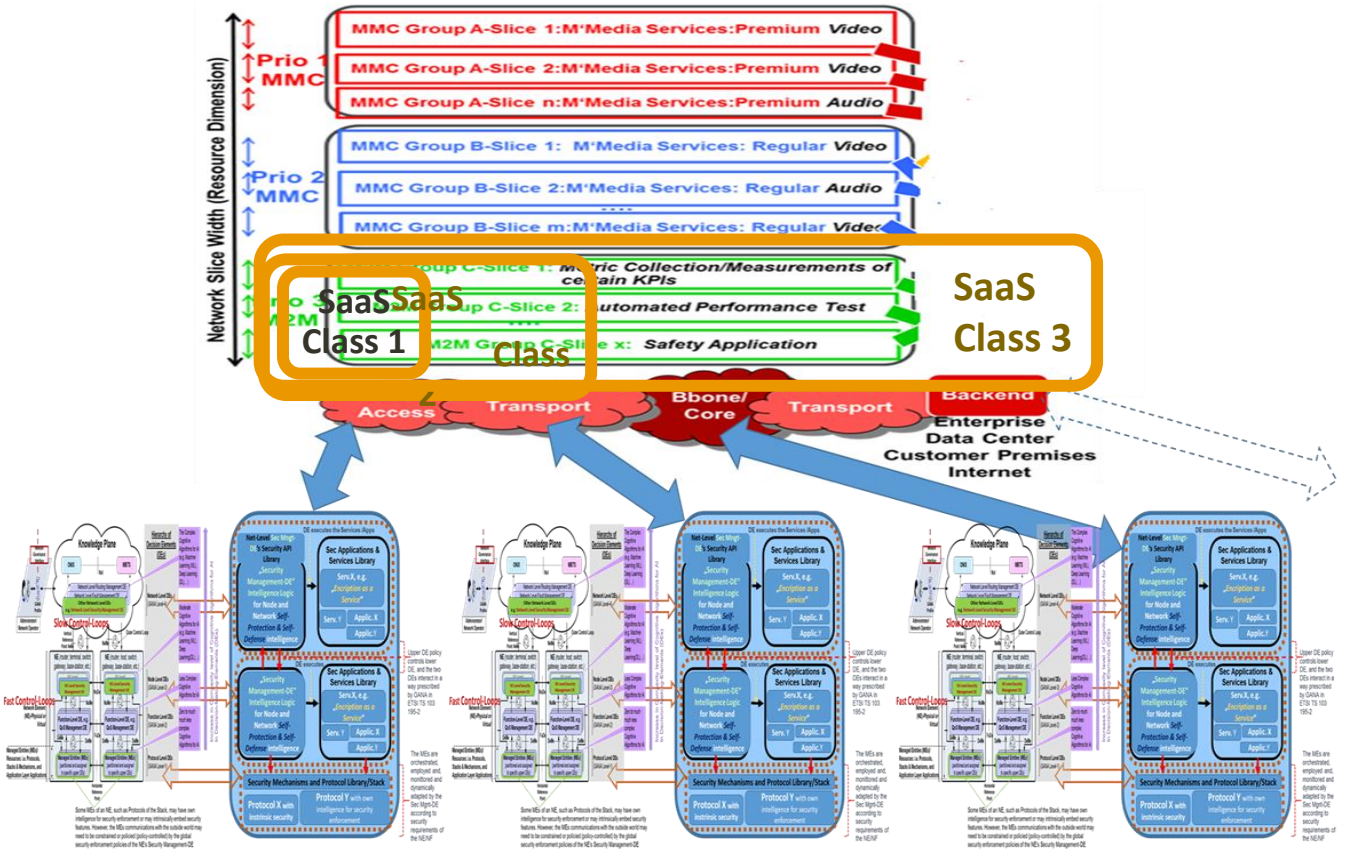
Class 2 SaaS: DDoS protection on UE and Network

Class 3 SaaS: DDoS Protection on UE and Network and Encryption of slice per Tier or/and E2E



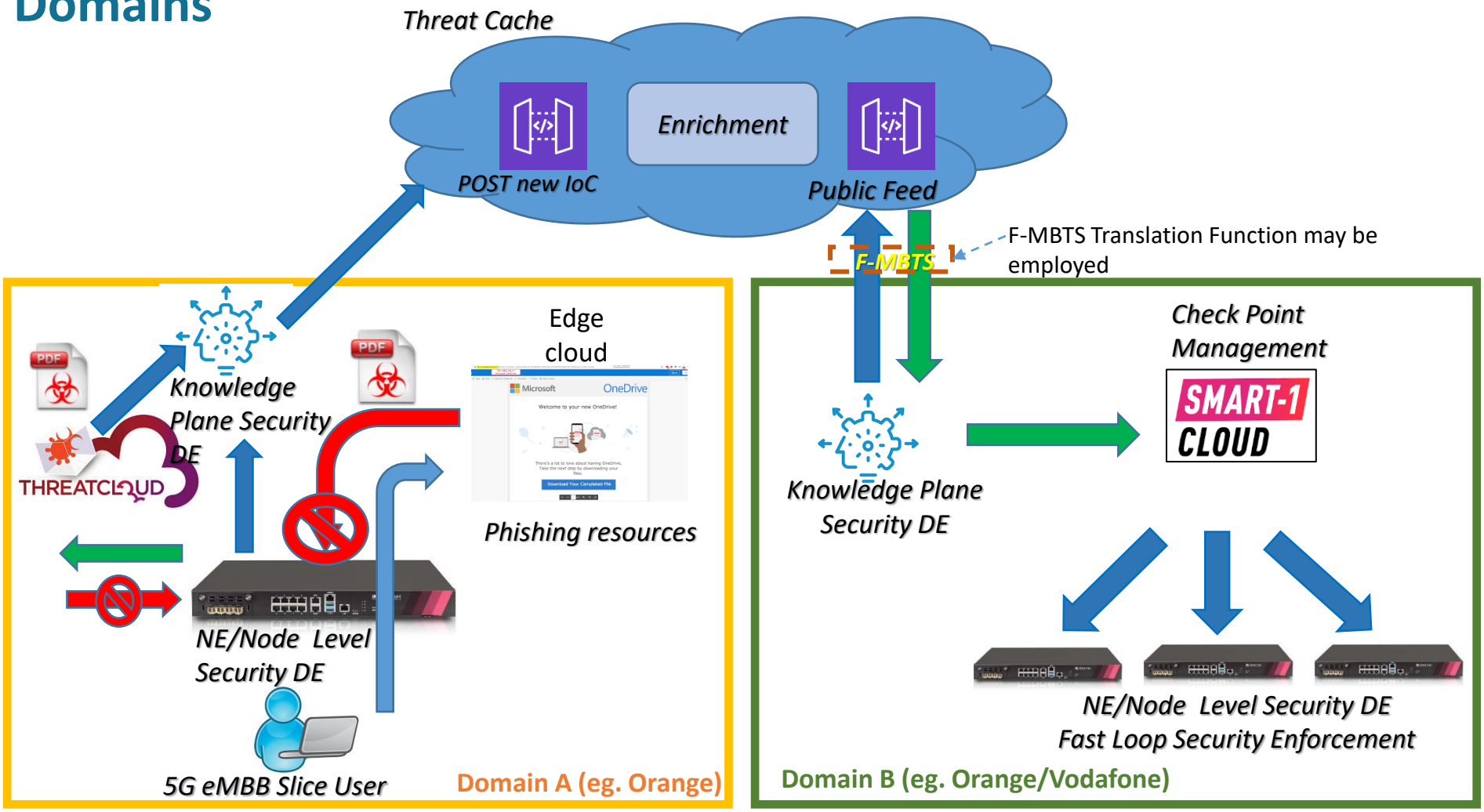
https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

SaaS Horizontal Segmentation



https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf

Threat Detection Info Dissemination (Federation) within the Same Operator Domain and to Other Collaboration Operator Domains



Thank You

Q & A

Demo: GANA Autonomics in SaaS SLA for

"Protection Class" in a 5G Slice: *Protection of Slice User/Consumer from Infected Documents meant to be downloadable or exchanged with Peers*

https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_6.pdf