ETSI GS NFV-IFA 026 V3.4.1 (2020-06)

Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/NFV-IFA026ed341

Keywords
architecture, management, MANO, NFV,
orchestration, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines the requirements to interface the Security Control to NFV-MANO as described in ETSI GS NFV-SEC 013 [1] and the LI Controller in ETSI GR NFV-SEC 011 [2]. The present document identifies the extensions to the NFV-MANO architecture related to security management and monitoring. Multiple trust domains are considered.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-SEC 013 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification".

[2] ETSI GR NFV-SEC 011 (V1.1.1): "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[3] ETSI GS NFV-SEC 012 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[4] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV-IFA 033: "Network Functions Virtualization (NFV) Release 4; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification".

[i.2] ETSI GS NFV 003 (V1.3.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.2] and the following apply:

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI GS NFV 003 [i.2].

security manager: function within an NFV network responsible for enforcing security policy for VNFs and for instructing NFV-MANO to take VNF specific or system wide security actions

NOTE: The security manager is a logical sub component of a CSP's overall network security management and monitoring systems.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.2] and the following apply:

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GS NFV 003 [i.2].

CSP	Communication Service Provider
HMEE	Hardware Mediated Execution Environment
NS	Network Service
NSD	Network Service Descriptor
SM	Security Manager
sNSD	security enhanced Network Service Descriptor
VSF	Virtual Security Function

4 Introduction

Within a CSP's network, it is necessary to be able to monitor and manage all components making up a network (including application layer software, NFVI software and hardware components). Therefore, a CSP's overall security management platform needs to have real-time access and understanding of NFV-MANO VNF orchestration and management events. In some scenarios it is sufficient to simply observe and alert on those events from a security perspective, while in other scenarios the CSP security management platform may be required to specifically authorize some or all actions undertaken by NFV-MANO. A CSP security management platform may require one or more Security Manager (SM) depending on the security isolation required between different trust domains.

ETSI GS NFV-SEC 013 [1] describes security management and monitoring in an NFV environment. The NFV SM as described in ETSI GS NFV-SEC 013 [1] is responsible for making security decisions associated with the instantiation, modification and termination of VNFs.

In order to achieve this the SM requires real-time information from NFV-MANO on VNF instantiation, modification and termination. This information needs to be sufficiently detailed for the SM to be able to resolve the type and version of a VNF(s) being instantiated, VNFD constraints applied to those VNFs, OSS/BSS application layer VNF(s) ID(s) (i.e. VNF instance name) and information about the intended physical hardware environment (host IDs/location, etc.). It is not important to the SM which NFV-MANO sub-components provide which specific pieces of information but it is important that the information is provided in an intelligible format. The SM is responsible for maintaining the cumulative state of the information received from NFV-MANO. However, in the case of SM failure or for state recovery under network/NFV-MANO failure conditions, it is desirable for NFV-MANO to be able to provide the SM with the current state of all VNFs (including hardware/resource usage and VNF and VNFCI interconnections routing table).

The SM is responsible for analysing information received from NFV-MANO and where necessary instructing NFV-MANO to take actions accordingly (e.g. applying security policy to a VNF being initiated). In addition, when the SM becomes aware of a security event (e.g. VNF compromise) the SM is responsible for instructing NFV-MANO to take appropriate mitigating actions (e.g. terminate a VNF instance or put a VNF into quarantine). NFV-MANO and wider network auto recovery mechanisms need to ensure that they are able to handle SM enforced VNF decisions and NFV-MANO does not attempt to restart or migrate VNFs that the SM has requested be terminated or quarantined.

In scenarios where there is not a single legal entity or CSP operating the entire virtual network (e.g. tenant hosted scenarios), the SM(s) implementation will need to ensure isolation of information, events or policy is maintained between different entities.

Where NFV-MANO has visibility of PNFs (e.g. by association with SDN routing to and from VNFs), that information also needs to be provided to the SM by NFV-MANO.

The present document contains set of requirements and analysis in annex A, for each of the reference points between NFV-MANO and the SM defined in clause 5. These requirements are derived from but not limited to those in ETSI GS NFV-SEC 013 [1].

5 Interface and Architectural Requirements

5.1 Functional blocks and reference points

Figure 5.1 shows the three new reference points and one new functional block which are required to be added to the underlying NFV architecture to support security monitoring and management, as defined in ETSI GS NFV-SEC 013 [1].

The new functional block is the Security Manager (SM). It may be necessary to have more than one Security Manager in order to meet all the security requirements, in which case each SM shall be handled independently within a separate trust domain using separate instances of endpoints on relevant interfaces defined over the three reference points. In the case of multiple security managers, each security manager may be authorized to perform different sub-sets of the requirements listed in annex A.

The three reference points are:

- Sc-Or: the reference point between the Security Manager and the NFV Orchestrator.
- Sc-Vnfm: the reference point between the Security Manager and VNF Manager.
- Sc-Vi: the reference point between the Security Manager and Virtualised Infrastructure Manager.

NOTE: The interfaces which run over these reference points are defined in ETSI GS NFV IFA 033 [i.1], which also contains requirements for those interfaces.

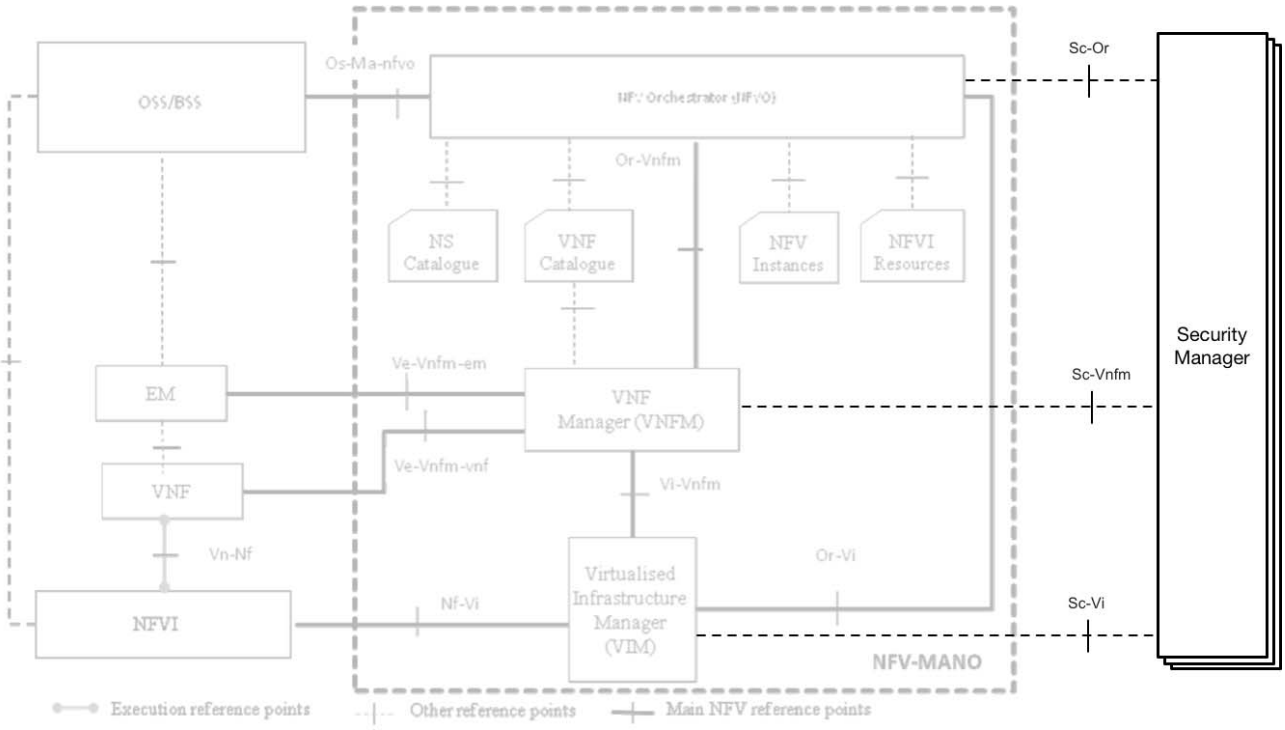

Figure 5.1: Security Manager and NFV-MANO Reference Architecture

5.2 SM Modes

The SM and NFV-MANO shall support three modes of operation:

- Passive: SM is able to subscribe to applicable lifecycle management events passed to it by NFV-MANO but the SM does not take any active part in the lifecycle management of the VNFs.
- Semi-Active: SM analyses applicable lifecycle management events passed to it by NFV-MANO. The SM may provide security policies to NFV-MANO as part of a VNF lifecycle management but the SM takes an otherwise passive part in VNF lifecycle management. The SM is able to request NFV-MANO to undertake security mitigation actions (e.g. terminate a VNF instance).
- Fully-Active: NFV-MANO passes applicable VNF lifecycle events to the SM and requests approval from the SM. The SM authorizes, modifies with security policy, or rejects NFV-MANO requests. The SM is also able to instruct NFV-MANO to take security mitigation actions (e.g. immediately terminate a VNF instance).

NOTE: The full scope of lifecycle events which are applicable to the SM in Passive, Semi-Active and Fully-Active modes are outside the scope of the present document. However, the applicability of specific VNF lifecycle management events would be determined based on the necessity to meet the requirements defined in clause 5 and annex A.

5.3 Multiple Trust Domains and Security Managers

In networks with multiple trust domains or where a CSP wishes to achieve security role separation, there may be one or more SMs. Each SM may operate in Passive, or Semi-Active or Fully Active mode as described in clause 5.2.

It shall be possible for the SMs to act independently of each other or for SMs to operate in a hierarchical arrangement where one SM may be able to issue VNF termination instructions across all trust domains of one or more sub SMs.

NOTE: In hierarchy terms, a sub SM is an SM which is overseen or controlled by another higher security level SM. For example, a sub SM in Semi-Active Mode may be subservient to a network wide Fully Active SM. The sub SM is able to fulfil its role autonomously but the higher-level SM would be able to overrule it at any time. NFV-MANO needs to be able to support such hierarchical models and provide interface instance isolation for such sub SM to SM relationships.

Each SM shall interface to NFV-MANO using a logically separate, dedicated instance of interfaces as defined in clause 5.1. Each set of SM to NFV-MANO interfaces shall use independent integrity and confidentially protection from all other SM to NFV-MANO interface sets.

NFV-MANO is responsible for ensuring that VNF lifecycle management events are sent to the correct one or more SMs subject to the trust domain separation model being implemented by a network.

NFV-MANO shall not accept instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain (hierarchical layering requirement above notwithstanding).

SM to NFV-MANO trust domain separation shall include support for management of sensitive components as defined in ETSI GS NFV-SEC 012 [3].

NFV-MANO shall support an authorization framework where each SM is authorized in Passive or Semi-Active or Fully-Active mode to undertake interactions with NFV-MANO.

Each SM to NFV-MANO authorization shall be independent of any other SM binding. NFV-MANO shall ensure that each SM is invisible to any other SM (hierarchical layering requirement notwithstanding).

Where one SM spans multiple trust domains, it shall be possible for the SM to operate in different modes (Passive, Semi-Active, Fully-Active) for each trust domain.

NFV-MANO shall be able to manage and authorize these different modes for different trust domain for a single SM independently.

The present document assumes that where more than one SM exist in an NFV implementation, one SM will act as a master SM such that is able to instruct NFV-MANO to immediately terminate any VNF belonging to any sub SM trust domain or over-rule the actions of a sub SM.

Where NFV-MANO is required to maintain audit logs of lifecycle managements events, NFV-MANO shall be able to separate these based on the SM and trust domain separation requirements above.

Detailed requirements for multiple trust domains and multiple SMs are defined in annex A.

Annex A (normative): Reference point functional requirements

A.0 General

This annex provides requirements to be supported by NFV-MANO over the three functional reference points identified in clause 5.1 and the consequential functional requirements on the NFV-MANO functional blocks terminating those reference points. Clause A.1 provides requirements derived directly from ETSI GS NFV-SEC 013 [1], while clause A.2 provides additional requirements to address areas which are not covered in ETSI GS NFV-SEC 013 [1] in sufficient detail.

A specific NFV-MANO and SM pairing will support a subset of these requirements depending on the operational deployment model and the role of the SM.

The requirements includes functionality required to support the LI Controller as specified in ETSI GR NFV-SEC 011 [2].

The assignment of specific requirements in this annex to one or more of the 3 functional reference points (Sc-Or, Sc-Vnfm, Sc-Vi) as described in clause 5, is provided in ETSI GS NFV-IFA 033 [i.1].

A.1 Requirements on security management and monitoring from ETSI GS NFV-SEC 013

The following requirements are derived from ETSI GS NFV-SEC 013 [1].

In ETSI GS NFV-SEC 013 [1], clause 6.5.1 "Requirements for Multi-Trust-Domain Security Management":

R1.1.10. Entities (e.g. VNFs) building up telco networks (e.g. IMS network) shall be assignable to different trust domains.

R1.1.20. One or more dedicated NFV-MANO trust domains shall exist.

R1.1.30. Each NFV-MANO functional block shall be assignable to one or more dedicated NFV-MANO trust domain(s).

R1.1.40. Trust relationships shall be defined between trust domains.

R1.1.50. For two or more domains without existing trust relationships, the effect of an attack on one domain shall not impact the other domains either directly or indirectly (e.g. through Management channels).

R1.1.60. MANO shall support one or more NFV SMs, per trust domain.

R1.1.70. There shall be controls enforcing separation of duties and privileges, least privilege use and least common mechanism between security management and NFV-MANO. These controls shall apply in conjunction with the corresponding separation of trust domains.

R1.1.80. A NFV SM shall manage security policies and implement the security requirements of a trust domain to be implemented by dedicated security functions or security functions embedded within VNFs.

R1.1.90. A SM shall manage security policies and requirements between trust domains according to the defined trust relationship, including establishing security association between VNFs in different trust domains and between VNFs and NFV-MANO entities when it has visibility and permissions available to perform such duties:

- Security policies reflecting trust relationships between trust domains could include access control (authentication and authorization), traffic/resource separation and segmentation, VPN SeGW, etc.

R1.1.100. A SM shall manage security policies within a trust domain, including establishing security association between VNFs within a single trust domain.

Security policies within each trust domain included e.g. initial key provisioning for secure communication between VNFs, authentication and authorization mechanisms, firewalls, etc.

R1.1.110. SMs shall be able to interact (where authorized) with each other for requesting/providing required security services for e.g. cross-domain security management.

R1.1.120. One or more dedicated trust domains for Security Management shall exist.

R1.1.130. SM shall be assignable to one of the dedicated Security Management trust domains.

R1.1.140. The SM shall be instantiated on a host system which meets the requirements laid out in ETSI GS NFV-SEC 012 [3].

R1.1.150. The SM may be deployed as virtualised workload.

R1.1.160. Traffic of SM shall be isolated and separated from other traffics in data/control planes, etc.

In ETSI GS NFV-SEC 013 [1], clause 6.5.2 "Requirements for Network Security Management":

R1.2.10. The NFV security management system shall support the security lifecycle management as introduced in ETSI GS NFV-SEC 013 [1], clause 6.1:

- The security management system shall support capabilities allowing operators to perform security policy planning for network services, which includes security policy initial design and optimization.
- The security management system shall support a capability allowing operators to enforce (including validate) the designed security policies throughout the network service lifecycle.
- The security management system shall support a capability allowing operators to perform security monitoring as described in ETSI GS NFV-SEC 013 [1], clause 7.

R1.2.20. The operator's security management system shall support a capability to manage security functions in both virtualised and physical networks within bounds of trust domains.

R1.2.30. The NFV security management system shall support a capability allowing operators to automate the security management functions.

R1.2.40. To facilitate security policy design, the SM shall support checking the availability and capabilities of VSFs and ISFs (via ISM), as well as PSFs (via the associated EM(s)).

R1.2.50. The SM shall support extending NSD with the security information contained in the designed security policies to create sNSD.

R1.2.60. The sNSD shall support the security zone/placement, the connectivity and the description of the VSFs needed for controlling the traffic to VNFs.

R1.2.70. The sNSD shall be made available to the NFVO for deploying network services with security protection.

R1.2.80. If sNSD is available before a network service is deployed, the sNSD shall be used by the NFVO for initial deployment of the network service. The VSFs (e.g. the virtual firewalls included in sNSD) for protecting the network service are instantiated together with the VNFs assigned to the network service.

R1.2.90. If sNSD is not available before a network service is deployed, the SM shall be able to get the information of the deployed network service (or VNFs) from the NFVO for applying security policies to the unprotected network service.

R1.2.100. To enforce security policies on unprotected network services, the SM shall be able to trigger the instantiation of the required VSF(s) (via the VNFM) according to the designed security policies and update network topology accordingly.

R1.2.110. For updating the enforced security policies when network services are scaled-in/scaled-out, the SM shall be informed (by the NFVO) of the result of the scaled network services.

R1.2.120. The SM shall be able to trigger the instantiation of new VSF(s) required for protecting the instantiated VNF(s) for scaled network service or termination of affected VSF(s) via the VNFM, based on the designed security policies.

R1.2.130. The SM shall have the capability to configure security rules on VSFs/PSFs (via the associated EMs) and ISFs (via ISM) following the designed security policies.

R1.2.140. Network Security Management shall provide an interface from the SM to the VSFs/PSFs (via the associated EMs) and ISFs (via ISM) to allow configuration of the instantiated VSFs (e.g. initial credentials, etc.).

R1.2.150. The SM shall have the capability to configure security policy validation for the deployed/scaled network services.

R1.2.160. Network Security Management shall provide an interface from the SM for security policy validation for the deployed/scaled network services.

R1.2.170. The SM shall have the capability to clean-up of enforced security policies related resources for the terminated network services.

In ETSI GS NFV-SEC 013 [1], clause 7.5 "NFV Security Monitoring & Management Requirements":

R1.3.10. Network monitoring solution shall not render vulnerable the security of the network or the user data any more than it is without the network monitoring solution in place.

R1.3.20. The monitoring solution in NFV shall provide an equivalent or higher level of security than the monitoring solutions in existing non-virtualised networks.

R1.3.30. Active Monitoring failures should be fail safe. Passive monitoring failures should be silent from user perspective.

R1.3.40. The Security Monitoring components should be protected from other NFV system components, and should execute in Hardware Mediated Execution Enclave (HMEE) within appropriate trust domains.

R1.3.50. Security Monitoring should not impact IaaS, PaaS, and SaaS SLAs, except as otherwise defined in the present document.

R1.3.60. Security Monitoring depends upon security requirements established by the ETSI GS NFV-SEC 001 [4], including Secure and Measured boot and establishing secure channels based on mutual authentication.

R1.3.70. A comprehensive deployment of Security Monitoring solution will monitor both virtualised and non-virtualised network functions.

R1.3.80. NFVI resource allocation and platform quality of service technologies should be put in place to ensure that the Security Monitoring functions are not starved of NFVI resources causing unexpected security consequences. Such mechanisms should reliably ensure that starvation and DoS attacks against Security Monitoring functions are minimized or eliminated.

R1.3.90. Security Monitoring components shall be securely provisioned within the system, which means that these systems will be provisioned for deployments in a trusted environment. This includes root key provisioning, setting up HMEE, certificate provisioning, etc.

R1.3.100. Security Monitoring components shall be booted using secured and measured boot technologies.

R1.3.110. Once Security Monitoring and Management systems are in place, these shall detect authorized and unauthorized on-boarding, deployments, activation, and run time integrity checking of VNFs.

R1.3.120. Once VNFs are deployed, Security Monitoring and Management System shall ensure that the security policies of the deployed VNFs are enforced.

R1.3.130. Security Monitoring systems shall protect Telemetry data-at-rest, both at local or remote secure storage.

R1.3.140. Security Monitoring telemetry may be compressed prior to storage and/or during transit.

R1.3.150. A Security Monitoring and Management system will ensure that the VNFs and SFCs have been securely configured, meaning that start-up and security enforcement policies (e.g. VNFDs, Configuration) were delivered to the VNFs in a protected manner. It is assumed that the configuration data itself is vetted and accurate, per the security policy.

R1.3.160. Once provisioned, Security Monitoring and Management system will ensure that the VNFs are not activated unless their security policy is addressed. For example, all VNFs in a SFC should be deployed prior to activation of a specific VNF.

R1.3.170. The Security Monitoring and Management system will help monitor VNF topology changes, including migration, scale-in, and scale-out of VNFs.

R1.3.180. Security Monitoring and Management will observe the VNFs instantiation and termination process and it should be able to detect and remediate improperly authorized actions.

R1.3.190. The Security Monitoring and Management system will help detect and remediate VNF exploits during the normal course of VNF's operational life-cycle. For instance, attacker could attempt to exploit a known vulnerability in a VNF, which can be detected and blocked by the security monitoring system.

R1.3.200. NFV Security Monitoring components should run in a HMEE.

R1.3.210. The NFV Security Monitoring and Management system shall ensure that all Security Monitoring services and policies are securely provisioned and activated prior to NFV system bring-up.

R1.3.220. NFV Security Monitoring and Management system shall interface with the NFV system life-cycle, including hardware, firmware, and software updates, to ensure that these are authorized and occur per security policy.

R1.3.230. Security Monitoring may perform Active and Passive Security Monitoring of the Control, Management, and Data planes in a VNF.

R1.3.240. Security Monitoring can be continuous, manual, or triggered by a specific set of events, as in automated anomaly detection. Monitoring can also be triggered by an administrator based on their specific criteria.

R1.3.250. NFV Security Monitoring system may securely distribute telemetry to multiple Security Monitoring Collection and Analytics Systems, based on the security policies for minimizing latencies associated with detection remediation of threats.

R1.3.260. Security Monitoring components should follow security best practices for auditing, including secure logging and tracing.

R1.3.270. Audit logs contain sensitive information, and based on security policy, Audit Log data-at-rest should be confidentiality and/or integrity protected with a securely provisioned key.

R1.3.280. The Audit Logs, in transit, should be integrity and confidentiality protected using pairwise unique keys.

R1.3.290. Network Monitoring should not lower the reliability of the system from its state prior to enabling Security Monitoring.

A.2 Additional Requirements

The following requirements are in addition to those derived from ETSI GS NFV-SEC 013 [1] in clause A.1 of the present document:

R2.1.10. NFV-MANO shall support SMs that are Passive, or Semi-Active or Fully Active as defined in clause 5.2.

R2.1.20. For SMs in Passive mode, NFV-MANO shall send applicable lifecycle management events to the SM but NFV-MANO shall not wait for the SM to provide any response to NFV-MANO, nor shall NFV-MANO accept requests to modify the VNF lifecycle.

R2.1.30. For SMs in Semi-Active mode, NFV-MANO shall send applicable lifecycle management events to the SM. For VNFs which require security policy management, the SM shall provide NFV-MANO with the necessary info and NFV-MANO shall act on it accordingly. However, in general NFV-MANO shall carry on with lifecycle management without SM intervention unless the SM responds negatively. SMs may request NFV-MANO to take lifecycle management action at any time.

R2.1.40. For SMs in Full-Active mode, NFV-MANO shall send applicable lifecycle management events to the SM. NFV-MANO shall not proceed with lifecycle management until the SM positively confirms permission and provides any security policy instructions. NFV-MANO shall immediately action instructions from an Active SM regardless of the impact on the network application layer services (e.g. immediately kill one or more VNFs).

NOTE 1: An SM fully implementing the requirements of ETSI GS NFV-SEC 013 [1], is a Fully-Active SM.

R2.1.50. NFV-MANO shall support hierarchical relationships for networks with multiple SMs or trust domains.

R2.1.60. NFV-MANO shall support a dedicated logical set of interfaces (as defined in clause 5.1) for each SM.

R2.1.70. NFV-MANO shall support separate independent security associations and keys for each SM on each logical interface.

R2.1.80. NFV-MANO shall ensure that only lifecycle management events applicable to a specific SM(s) are sent to that SM(s).

R2.1.90. NFV-MANO shall not accept instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain.

R2.1.100. SM to NFV-MANO trust domain separation shall include support for management of sensitive components as defined in ETSI GS NFV-SEC 012 [3].

R2.1.110. NFV-MANO shall support an authorization framework where each SM is authorized in Passive or Semi-Active or Fully-Active mode to undertake interactions with NFV-MANO.

R2.1.120. Each SM to NFV-MANO authorization shall be independent of any other SM binding and NFV-MANO shall ensure that each SM is invisible (if required) to any other SM.

R2.1.130. Where one SM spans multiple trust domains, it shall be possible for the SM to have different modes (Passive, Semi-Active, Fully-Active) for each trust domain.

R2.1.140. Where one SM has multiple modes for different trust domains, NFV-MANO shall be able to manage and authorize these rolls independently.

R2.1.150. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is created.

R2.1.160. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is modified. Modification is any change to a VNF but not limited to:

- configuration;
- run-time images or code version;
- location (physical or logical);
- host resources;
- NFV layer communications peering relationships (including PNFs where visible to NFV-MANO);

- identification;
- changes to one or more VNFCI with a VNF;
- load balancing;
- any other change which could have an impact on security policy or management.

R2.1.170. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is terminated, crashes or ceases to exist for any reason.

R2.1.180. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide information on the source of the VNF lifecycle management event (e.g. application layer OSS/BSS, VNF, EMs, auto healing function, etc.).

R2.1.190. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide information on the reason for the VNF lifecycle management event (e.g. new VNF instance requested).

R2.1.200. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide the ability to hide specific lifecycle events for sensitive functions as specified in ETSI GS NFV-SEC 012 [3] from one or more SMs.

R2.1.210. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide as a minimum the following information in a VNF instantiation event:

- Source of request (e.g. OSS/BSS or NFV-MANO automated process).
- VNF Package Identifier.
- VNFD Identifier.
- VNFD (if required by SM).
- Integrity checksum of VNF package (including indication of pass or fail from NFV-MANO perspective).
- MANO Reference Identifier for VNF instance being created.
- Requestor Reference Identifier used for VNF instance being created (e.g. OSS/BSS application layer VNF ID).
- SDN Connectivity information (including PNFs) as known by NFV-MANO.
- Group reference (e.g. NS ID) for VNFs being created as part of a VNFD or Orchestration request.
- Intended host(s) and physical location(s) of VNF.

R2.1.220. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide as a minimum the following information in a VNF modification event:

- Source of request.
- Reason for modification.
- Reference identifier for VNF Instance being modified.
- Details of the change.

R2.1.230. NFV-MANO shall provide as a minimum the following information in a VNF termination event:

- Source of request.
- Reference identifier for VNF Instance being terminated.
- Reason for termination.

R2.1.240. NFV-MANO shall be able to provide SM(s) with information to understand the context of lifecycle events.

R2.1.250. Where a VNF package has been signed, NFV-MANO shall provide the package integrity information for the VNF being created. For Semi-Active and Fully-Active SMs, the SM shall verify the package integrity and provide a confirmation to NFV-MANO. The start-up integrity check for sensitive components described in ETSI GR NFV-SEC 011 [2] shall be supported.

R2.1.260. If NFV-MANO receives a VNF termination request from a semi-active SM, NFV-MANO shall initiate automated termination of the VNF and associated service chain. NFV-MANO shall inform the OSS/BSS before terminating the VNF but shall not seek permission to terminate:

- The SM shall be able to specify to NFV-MANO whether another VNF instance may be created to replace the VNF being terminated.
- The SM shall be able to specify to NFV-MANO whether it wants a copy of the VNF to be quarantined for later analysis.
- The SM shall be able to specify to NFV-MANO whether other recovery action may be performed in relation to the terminated VNF instance.

R2.1.270. If NFV-MANO receives a VNF termination instruction from a fully-active SM, NFV-MANO shall immediately terminate the VNF instance. NFV-MANO shall not inform the OSS/BSS before terminating the VNF instance:

- The SM shall be able to specify to NFV-MANO whether another VNF instance may be created to replace the VNF instance being terminated.
- The SM shall be able to specify to NFV-MANO whether it wants a copy of the VNF instance to be quarantined for later analysis.
- The SM shall be able to specify whether the VNF image and VNFD can be reused for new VNF instances or should also be quarantined.
- The SM shall be able to specify whether the host should be made available for use by other VNF instances or should also be quarantined.
- The SM shall be able to specify to NFV-MANO whether other recovery action may be performed in relation to the terminated VNF instance.
- The SM shall be able to specify whether all other VNF instances running on the same host should be terminated.
- The SM shall be able to specify whether NFV-MANO shall actively erase all HMEEs, HSMs or other storage used by the terminated VNF instance, in addition to normal NFV-MANO routine resource re-use procedures.

R2.1.280. When a fully-active SM or semi-active SM instructs/requests termination of one or more VNF instances, the SM shall provide NFV-MANO with a list of VNF instances to be terminated.

R2.1.290. MANO shall support VNF termination requests/instructions using lists of VNF instance identifiers based on NFV-MANO managed IDs.

R2.1.300. MANO shall provide sufficient OSS/BSS application ID information to the SM so that SM is able to understand the mapping between VNF lifecycle events and the equivalent OSS/BSS application IDs.

R2.1.310. An SM shall be able to provide NFV-MANO with security policy management instructions during a VNF lifecycle event or at any other time required by the SM.

NOTE 2: Content or format of the security policy information is outside the scope of the present document.

R2.1.320. A Semi-Active SM shall be able to request NFV-MANO to terminate the use of a specific host:

- The SM shall be able to specify to NFV-MANO whether VNF instances running on the host can be migrated or shall be terminated.

- The SM shall be able to specify to NFV-MANO whether to quarantine the host along with the hosted VNF instances.

R2.1.330. A Fully-Active SM shall be able to instruct NFV-MANO to immediately terminate the use of a specific host:

- The SM shall be able to specify to NFV-MANO whether VNFs running on the host can be migrated or shall be terminated.
- The SM shall be able to specify to NFV-MANO whether to quarantine the host along with the hosted VNFs.

R2.1.340. Semi-Active and Fully-Active SM shall be able to request instantiation, modification or termination of security functions to be inserted into or removed from the network service (e.g. between any two VNF instances or between sub-components within a single VNF instance) either as part of the NFV-MANO lifecycle management events notified by NFV-MANO to the SM(s) or at any other time required by the SM.

R2.1.350. An SM shall be able to request a network status list for all active VNF instances under control of NFV-MANO for that trust domain.

R2.1.360. An SM shall be able to request from NFV-MANO a list of VNF instances and their lifecycle history which previously existed in the network over a requested time period.

NOTE 3: The level of information required and period for which data should be held is outside the scope of the present document. However, the information retained needs to be sufficient to allow after the event network forensics over a reasonable timescale to be performed where a persistence attack has penetrated the network but the VNF instance or host which was compromised is no longer active.

Annex B (informative): Change History

Date	Version	Information about changes
2016-11	0.1.0	Implemented NFVIFA#40 approved contributions NFVIFA(16)0001320r1, NFVIFA(16)0001334 and NFVIFA(16)0001380r2.
2017-05	0.2.0	Implemented NFVIFA#52 approved contribution NFVIFA(17)000315.
2017-08	0.3.0	Implemented approved contribution NFVIFA(17)000500.
2018-09	0.4.0	Major re-write of document to align with transfer of document ownership to NFV SEC. Output of SEC in NFV SEC#131 F2F as SEC(18)000111. This version entirely replaces all sections of v0.3.0.
2018-12	0.5.0	Output from SEC#136F2F. Includes NFVSEC(18)000138r3.
2019-02	0.5.1	Editorial formatting and drafting rule corrections.
2019-02	0.5.2	Implementing comments in NFVIFA(19)000161r1 and some comments in NFVIFA(19)000162.
2019-02	0.5.2a & b	Address comments in NFVIFA(19)000156r1.
2019-03	0.6.0	Agreed baseline at NFVSEC#142. Content same as v0.5.2b.
2019-05	0.6.1	Drafting rule compliance ("must" replaced in Notes).
2019-05	0.6.2	Further final review comments addressed (see IFA/SEC email lists).
2020-06	3.4.1	Publication (unmodified with respect to version V3.2.1).

History

Document history		
V3.2.1	July 2019	Publication
V3.4.1	June 2020	Publication