# RM and RA-1: ONAP Security Requirements

> ⚠️ This page will serve as a placeholder to get the matrix complete and then the Recommended changes will be made to RM Chapter 07 and RA_1 Chapter 02. On completion of those adds this page will be archived.

## ONAP Security Requirements

| | ONAP Security Ref | Description | Notes | | CNTT Relevant | Exists | CNTT Ref# | Current Description, if exists | Recommended Description (may be a modification of existing) | Notes |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | SECCOM-103 | ONAP MUST implement and enforce the principle of least privilege on all protected interfaces. | | | Y | Y | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control) | | |
| 2 | SECCOM-114 | ONAP MUST provide a mechanism (e.g., access control list) to permit and/or restrict access to services on ONAP by source, destination, protocol, and/or port. | | | Y | Y | multiple | | The Platform **MUST** provide a mechanism (e.g., access control list) to permit and/or restrict access to platform services by source, destination, protocol, and/or port. | Propose adding this explicit |
| 3 | SECCOM-115 | ONAP SHOULD provide a mechanism that enables the operators to perform automated system configuration auditing at configurable time intervals. | | | Y | N | | | The Platform **SHOULD** provide a mechanism that enables the operators to perform automated system configuration auditing at configurable time intervals. | |
| 4 | SECCOM-116 | ONAP SHOULD provide the capability for the Operator to run security vulnerability scans of the operating system and all application layers. | | | Y | N | | | The Platform **SHOULD** provide the capability for the Operator to run security vulnerability scans of the operating system and all application layers. | Proposal to modify "all application layers" by "Platform application layers" in order to exclude the workloads. It can be added in System Hardening |
| 5 | SECCOM-117 | ONAP SHOULD have source code scanned using scanning tools (e.g., Fortify) and provide reports. | | | N | | | | | Image, log files and other scanning included in CNTT Reqts |
| 6 | SECCOM-118 | ONAP MUST have all code (e.g., QCOW2) and configuration files (e.g., HEAT template, Ansible playbook, script) hardened, or with documented recommended configurations for hardening and interfaces that allow the Operator to harden ONAP. Actions taken to harden a system include disabling all unnecessary services (eg, listening ports), removing unnecessary programs (eg. compilers, testing tools, password crackers, port scanners, sample programs) and changing default values. | | | Y | Y | sec.gen.004 | The Operating Systems of all the servers part of Cloud Infrastructure **must** be hardened by... | | for relevant components |
| 7 | SECCOM-119 | Traffic of the ONAP internal APIs MUST be possible to be isolated from traffic of the ONAP external APIs | | | Y | Y | sec.sys.001 to sec.sys.004 | | | OSTK intrinsic |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | SECCOM-119 | Network isolation capability between the traffic of different ONAP external APIs MUST be supported. The capability to isolate ONAP NBI traffic from all other external traffic MUST be supported. | | | Y | Y | sec.sys.004 | The Cloud Infrastructure **must** support Secure network channels | | |
| | | | | | | | sec.sys.005 | The Cloud Infrastructure **must** segregate the underlay and overlay networks | | |
| | | | | | | | sec.sys.002 | The Platform **must** support Traffic Filtering for workloads (for example, Fire Wall) | | |
| 9 | SECCOM-119 | All the ONAP network isolation mechanisms MUST be operator configurable. | | | N | N | | | | |
| 10 | SECCOM-120 | ONAP SHOULD support network segregation on ONAP internal interfaces: both between and inside the Kubernetes cluster(s). This means isolation of the internal APIs with different types of traffic (like: DB traffic, monitoring traffic, ...). | The separation is realized e.g., using network namespaces and K8s network policies. It must be carefully considered if multiple applications can be deployed in one K8s cluster, if the network segregation by namespaces and policies alone is sufficient - or if separation to different machines / VMs is required for increased security. | | | | | | | |
| 11 | SECCOM-121 | ONAP SHOULD be compatible with HW assisted security technologies like HSM, secure enclaves, TPM / virtual TPM for protection of more critical data (like encryption keys, secrets). | | | Y | Y<br><br>Partial | sec.sys.012 | The Platform **must** only use secrets encrypted using strong encryption techniques, and stored externally from the component | | 1. The Notes mentions Barbican. Should it mention HSM and TPM It could be added but in "should" recommendation. In RM Should reco to be added to refer to 7.6.5<br>2. Should there be a similar requirement for workloads? |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 12 | SECCOM-122 | ONAP MUST have patches available for vulnerabilities in ONAP aligned with CII badging specifications of criticality & delivery time. | Link to the CII requirement: https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/criteria.md | | Y | Y | sec.lcm.011<br><br>sec.lcm.017 | The Platform **must** implement Security life cycle management processes including proactively update and patch all deployed Cloud Infrastructure software.<br><br>The Platform must Audit systems for any missing security patches and take appropriate actions | |
| 13 | SECCOM-123 | ONAP MUST support encrypted access protocols, following the current best practices in: https://wiki.onap.org/display/DW/Recommended+Protocols | | | Y | Y | sec.sys.003<br><br>sec.lcm.002 | The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic<br><br>Operational (Typo ??) (Operations) **must** use management protocols limiting security risk such as SNMPv3, SSH v2, ICMP, NTP, syslog and TLS v 1.2 or higher. | Suggest Add another requirement:<br><br>The Platform **must** support encrypted access protocols such as TLS1.2 and newer or better.<br><br> Yes,described in 6.3.3.1<br><br>When using TLS protocols, the Platform **must** choose an encryption cipher that supports PFS. In the list of ciphers found in https://www.owasp.org/index.php/TLS_Cipher_String_Cheat_Sheet choose only ciphers in the A+, A or B category.<br><br>All web pages **must** be served over HTTPS and the HTTP Strict Transport Security (HSTS) policy must be preloaded on the browsers. | |
| 14 | SECCOM-124 | ONAP MUST store Authentication Credentials used to authenticate to other systems encrypted except where there is a technical need to store the password unencrypted in which case it must be protected using other security techniques that include, but are not limited to, the use of file and directory permissions. | | | Y | Y | sec.sys.012 | The Platform **must** only use secrets encrypted using strong encryption techniques, and stored externally from the component | |
| 15 | SECCOM-125 | For all GUI and command-line interfaces, ONAP MUST provide the ability to present a configurable warning notice. A warning notice is a formal statement of resource intent presented to everyone who accesses the system. | | | N | N | | | |
| 16 | SECCOM-126 | ONAP MUST allow the Operator to disable or remove any security testing tools or programs included in ONAP, e.g., password cracker, port scanner. | | | N | N | | | |
| 17 | SECCOM-127 | ONAP MUST define all the access points. | | | Y | Y | sec.sys.001 | The Platform **must** support authenticated and secure APIs, API endpoints<br><br>The Platform **must** implement authenticated and secure access to GUI | |
| 18 | SECCOM-127 | ONAP MUST enforce authorization on all the access points, and/or give recommendations for the ONAP deployment to enforce in the Kubernetes platform and Rancher. | | | Y | Y | sec.sys.001 | The Platform **must** support authenticated and secure APIs, API endpoints | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 19 | SECCOM-128 | ONAP MUST log any security event required by ONAP Requirements to Syslog and give the user the ability to configure LOG_AUTHPRIV or LOG_AUTH as needed. | can only know if it is a security event after analysis | | Y | Y | sec.gen. 015<br><br>+<br><br>sec.mon. 005, sec. mon.006<br><br>sec.mon. 08 to sec. mon.12 | Any change to the Platform must be logged as a security event, and the logged event must include the identity of the entity making the change, the change, the date and the time of the change. | | multiple |
| 20 | SECCOM-129 | ONAP MUST be operable without the use of Network File System (NFS). | | | N | | | | | |
| 21 | SECCOM-130 | ONAP MUST NOT contain any backdoors. | | | Y | N | | | PR#2081<br><br>New sec.sys.015:<br><br>The platform **must not** contain back door entries (unpublished access points, APIs, etc.) | Notes from RA1 meeting Oct. 19th:<br><br>Already tested by RC2<br><br>Nothing in OpenStac k, but can be done<br><br>CIS benchmar k? |
| 22 | SECCOM-131 | If SNMP is utilized, ONAP MUST support the most recent secure version of SNMP with message authentication. | | | Y | Y | sec.lcm. 002 | | | general requireme nt to have latest security patches for all componen ts |
| 23 | SECCOM-132 | ONAP application processes MUST NOT run as root. | | | N | | | | | "OpenStac k services generally run under a specific, unprivilege d user. However, sometimes they need to run a command as root."<br><br>"All nodes wishing to run nova-rootwrap should contain a sudoers entry that lets the unprivilege d user run nova-rootwrap as root, pointing to the root-owned ro otwrap. conf configurati on file." |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 24 | SECCOM-133 | Login access (e.g., shell access) to running instance of ONAP components, whether interactive or as part of an automated process, MUST be through an encrypted protocol such as SSH or TLS. | | | Y | N | sec.lcm.002 partial coverage | | PR#2081 New sec.sys.016: Login access to the platform's components must be through encrypted protocols such as SSH v2 or TLS v1.2 or higher Note: hardened jump servers isolated from external networks are recommended. | Notes from RA1 meeting Oct. 19th: Https for OpenStack End Points, self signed certificates not allowed ->RA1 "should" or "must"? Private EP /Public EP Check the latest ONAP version |
| 25 | SECCOM-134 | ONAP MUST, after a successful login at command line or a GUI, display the last valid login date and time and the number of unsuccessful attempts since then made with that user's ID. This requirement is only applicable when the user account is defined locally in ONAP. | | | N | | | | | OSTK GUI (Horizon) provides this |
| 26 | SECCOM-135 | ONAP MUST include a configuration that specifies the targetted parameters, e.g. a limited set of ports, over which ONAP run-time is accessed from (like: from ONAP design-time and ONAP north-bound interfaces). | | | N | | | | | |
| 27 | SECCOM-135 | ONAP MUST include a configuration that specifies the targetted parameters, e.g. a limited set of ports, over which ONAP design-time is accessed from (like: from ONAP north-bound interfaces). | | | N | | | | | OpenStack has default ports for each of its services |
| 28 | SECCOM-136 | ONAP MUST support the creation of multiple unique IDs so that individual accountability can be supported. | | | N | | | | | |
| 29 | SECCOM-137 | ONAP MUST support a flexible mechanism to assign permissions to each user ID (human or system). | | | N | | | | | OpenStack RBAC where needed |
| 30 | SECCOM-138 | Each ONAP component MUST support access restriction independently of other components. | | | Y | Y | sec.sys.001 | The Platform **must** support authenticated and secure access to API, GUI and command line interfaces. | | OpenStack Intrinsic |
| 31 | SECCOM-139 | ONAP MUST NOT allow the assumption of the permissions of another account to mask individual accountability. | | | N | | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control). | | sec.sys.007 does not cover individual accountability, but is sufficient for a common set of requirements |
| 32 | SECCOM-140 | ONAP MUST set the default settings for user access to deny authorization, except for a super user type of account. When ONAP is installed, nothing should be able to use it until the super user configures ONAP to allow other users (human and application) have access. | | | N | | | | | |
| 33 | SECCOM-141 | ONAP MUST support strong authentication, also known as multifactor authentication, on all protected interfaces exposed by ONAP for use by human users. Strong authentication uses at least two of the three different types of authentication factors in order to prove the claimed identity of a user. | removed Although ONAP has removed shouldn't CNTT require it. "Should" rather than "must" | | | | | | | |
| 34 | SECCOM-142 | ONAP MUST disable unnecessary or vulnerable cgi-bin programs. | removed: covered by another requirement | | | | | | | |
| 35 | SECCOM-143 | ONAP MUST provide access controls that allow the Operator to restrict access to ONAP functions and data to authorized users. | | | Y | Y | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control) | | |

| # | ID | Requirement | Notes | | | | | | | Reference |
|---|---|---|---|---|---|---|---|---|---|---|
| 36 | SECCOM-144 | ONAP MUST support OAuth 2.0 authorization using an external Authorization Server. | | | N | | | | | OpenStack Keystone API v3 supports OAuth1 and has an extension to support OAuth2.0 |
| 37 | SECCOM-145 | ONAP MUST, if not integrated with the Operator's Identity and Access Management system, support configurable password expiration. | removed: Authentication is not in the scope of ONAP, but shall be externalized. And, Exception: the ONAP super-user default account. For this, no password expiration should be defined. Although ONAP has removed shouldn't CNTT require it. Integration with an external IAM is privileged, so it is not useful to adress this point | | N | | | | | |
| 38 | SECCOM-146 | ONAP MUST support Role-Based Access Control to enforce least privilege. | | | Y | Y | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control) | | |
| 39 | SECCOM-147 | ONAP MUST, if not integrated with the Operator's Identity and Access Management system, comply with "password complexity" policy. When passwords are used, they shall be complex and shall at least meet the following password construction requirements: (1) be a minimum configurable number of characters in length, (2) include 3 of the 4 following types of characters: upper-case alphabetic, lower-case alphabetic, numeric, and special, (3) not be the same as the UserID with which they are associated or other common strings as specified by the environment, (4) not contain repeating or sequential characters or numbers, (5) not to use special characters that may have command functions, and (6) new passwords must not contain sequences of three or more characters from the previous password. | removed: Authentication is not in the scope of ONAP, but shall be externalized. And, Exception: the ONAP super-user default account. Although ONAP has removed shouldn't CNTT require it. Already covered by sec. gen002 with the reference to CIS Password Policy Guide, https://www.cisecurity.org/white-papers/cis-password-policy-guide, | | | Y | sec.gen.002 | All systems part of Cloud Infrastructure **must** support password hardening as defined in CIS Password Policy Guide https://www.cisecurity.org/white-papers/cis-password-policy-guide. | | |
| 40 | SECCOM-148 | ONAP MUST support deployment-time generation of passwords for internal components or applications which do not support certificate based authentication or external IdP. | | | ? | Y | sec.sys.013 | The Platform **must** provide secrets dynamically as and when needed. | | |
| 41 | SECCOM-149 | ONAP MUST, if not integrated with the Operator's Identity and Access Management system, support the ability to disable the userID after a configurable number of consecutive unsuccessful authentication attempts using the same userID. | removed: Authentication is not in the scope of ONAP, but shall be externalized. And, Exception: the ONAP super-user default account. Although ONAP has removed shouldn't CNTT require it. If we privilege an external IAM, it is not useful to adress this point | | | | | | | |
| 42 | SECCOM-150 | ONAP MUST, if not integrated with the Operator's identity and access management system, authenticate all access to protected GUIs, CLIs, and APIs. | removed: Is covered by the requirement SECCOM-143 | | | | | | | |
| 43 | SECCOM-151 | ONAP MUST integrate with following standard identity provider protocols: LDAP, OpenID Connect and SAML authentication. | | | N | Y RA1 | | | | Per RA1 meeting Oct.19th Not for RM,but relevant for RA OpenStack supports integration with LDAP, OpenID and SAML |

| 44 | SECCOM-152 | ONAP MUST have the capability of allowing the Operator to create, manage, and automatically provision user accounts using an Operator approved identity lifecycle management tool using a standard protocol. | removed: Authentication is not in the scope of ONAP, but shall be externalized. And, Exception: the ONAP super-user default account. For this, no password expiration should be defined. Although ONAP has removed shouldn't CNTT require it. Covered by sec.sys.006 | | | | sec.sys.006 | The Cloud Infrastructure must be able to utilize the Cloud Infrastructure Manager identity lifecycle management capabilities. | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 45 | SECCOM-153 | ONAP MUST support account names that contain at least A-Z, a-z, 0-9 character sets and be at least 6 characters in length. | removed: Authentication is not in the scope of ONAP, but shall be externalized. And, Exception: the ONAP super-user default account. For this, no password expiration should be defined. Although ONAP has removed shouldn't CNTT require it. Same as #41 | | | | | | | |
| 46 | SECCOM-154 | For cases where ONAP is involved in the authentication process, eg LDAP: A failed authentication attempt MUST NOT identify the reason for the failure to the user, only that the authentication failed. | | | N | N | | | | |
| 47 | SECCOM-155 | ONAP MUST NOT display "Welcome" notices or messages that could be misinterpreted as extending an invitation to unauthorized users. | | | N | N | | | | |
| 48 | SECCOM-156 | ONAP MUST provide a means for the user to explicitly logout, thus ending that session for that authenticated user. | | | N | | | | | OpenStack Horizon including automatic logout |
| 49 | SECCOM-157 | ONAP MUST enforce a configurable "terminate idle sessions" policy by terminating the session after a configurable period of inactivity. Access token represents a session. | | | N | | | | | currently under Recommendations – compliance with standards Not for RM, For CNTT, does it concern workloads or can it apply to the platform's components? |
| 50 | SECCOM-158 | ONAP SHOULD integrate with the Operator's authentication and authorization services. | | | N | | | | | |
| 51 | SECCOM-159 | Each ONAP API MUST check the size (length) of all input. Do not permit an amount of input so great that it would cause the ONAP component to fail. Where the input may be a file, ONAP API must enforce a size limit. | | | N | | | | | |
| 52 | SECCOM-160 | Each ONAP API MUST NOT permit input that contains content or characters inappropriate to the input expected by the design. Inappropriate input, such as SQL expressions, may cause the system to execute undesirable and unauthorized transactions against the database or allow other inappropriate access to the internal network (injection attacks). | | | N | | | | | |
| 53 | SECCOM-161 | Each ONAP API MUST verify the format of the input files. No assumptions can be made based on MIME type nor file extension, other than indicating the expected type. | | | N | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 54 | SECCOM-162 | ONAP MUST be able to provide the ONAP related security events to an external system | | | Y | N | | | SECCOM-162 + SECCOM-182 + SECCOM-185<br><br>PR #2081<br><br>sec.mon.018<br><br>The platform, starting from initialization, must collect and analyze logs to identify security events, and store these events in an external system. | Requirements for collecting and analysis of logs, and corrective actions<br><br>1- Collect events<br><br>2- Analyze and sort events, identify security events (ref?, list?)<br><br>3- Store event in a central external system |
| 55 | SECCOM-162 | ONAP MUST be able to collect the security events from SW defined networks that it orchestrates | | | N | | | | | Knowing that something is a security event happens post-analysis |
| 56 | SECCOM-163 | ONAP MUST support Integration functionality via API /Syslog/SNMP to SIEM. | | | N | | | | | |
| 57 | SECCOM-164 | ONAP MUST support API-based monitoring to take care of the scenarios where the control interfaces are not exposed, or are optimized and proprietary in nature. | removed: every ONAP application should support a healthcheck API. But that is not seen as security related.<br><br>Although ONAP has removed shouldn't CNTT require it. | | N | | | | | |
| 58 | SECCOM-165 | ONAP MUST support detection of malformed packets, and generate an error message. | | | N | | | | | |
| 59 | SECCOM-166 | ONAP MUST support proactive monitoring to detect and report the attacks on resources so that ONAPs and associated VMs can be isolated, such as detection techniques for resource exhaustion, namely OS resource attacks, CPU attacks, consumption of kernel memory, local storage attacks. | | | Y | Y | sec.mon.011<br><br>sec.mon.009 | | | collection and analysis support this<br><br>Sec.mon.011 can be more precise |
| 60 | SECCOM-167 | ONAP SHOULD operate with anti-virus software which produces alarms every time a virus is detected. | | | | | | | | |
| 61 | SECCOM-168 | ONAP MUST protect all security audit logs (including API, OS and application-generated logs), security audit software, data, and associated documentation from any modification or unauthorized viewing. For example by OS access control mechanisms like file permissions, by sending to a remote system, or by encryption. | | | Y | Y | sec.mon.004 | The Platform must secure and protect Audit logs (contain sensitive information) both in-transit and at rest | | multiple requirements |
| 62 | SECCOM-169 | ONAP MUST at a minimum log the following: successful and unsuccessful authentication attempts, authentication associated with a transaction, authentication to create a session, authentication to assume elevated privilege. | | | Y | Y | sec.mon.005<br><br><br><br>sec.mon.006 | The Platform must Monitor and Audit various behaviours of connection and login attempts to detect access attacks and potential access attempts and take corrective actions accordingly<br><br>The Platform must Monitor and Audit operations by authorized account access after login to detect malicious operational activity and take corrective actions accordingly | | |
| 63 | SECCOM-170 | ONAP MUST log logoffs | | | N | | | | | |
| 64 | SECCOM-171 | ONAP MUST log starting and stopping of security logging. | | | N | | | | | |

| # | ID | Requirement | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 65 | SECCOM-172 | ONAP MUST log success and unsuccessful creation, removal, or change to the inherent privilege level of users. | | | Y | N | | | **PR#2081** <br><br> **Sec.lcm.012** <br><br> The platform must log any privilege escalation | Requirement: Log privilege escalation |
| 66 | SECCOM-173 | ONAP MUST log connections to the network listeners of the resource | | | N | | | | | |
| 67 | SECCOM-174 | ONAP MUST log the following fields in the security audit logs:<br>- event type<br>- date/time<br>- protocol<br>- service or program used for access<br>- success/failure<br>- Login ID<br>- source IP address | | | Y | N | | | PR#2081 <br><br> Addition to **Sec.mon. 001** <br><br> The platform's components must log the following fields in the security audit logs: <br><br> - event type<br> - date/time<br> - protocol<br> - service or program used for access<br> - success/failure<br> - Login ID or process ID<br> - IP address and ports (source and destination) involved | Requirement to be added to list all mandatory fields part of a logged event |
| 68 | SECCOM-175 | ONAP MUST NOT include an authentication credential, e.g., password, in any logs, even if encrypted. | | | Y | N | | | PR#2081 <br><br> Sec.mon.019 <br><br> The platform's components must not include an authentication credential, e.g., password, in any logs, even if encrypted. | Requirement to be added |
| 69 | SECCOM-176 | ONAP MUST detect when its security audit log storage medium is approaching capacity (configurable) and issue an alarm. | | | Y | Y | sec.mon. 015 | The Platform **must** ensure that the Monitoring systems are never starved of resources. | PR#2081 <br><br> Sec.mon.015 modified by: <br><br> The Platform **must** ensure that the Monitoring systems are never starved of resources and **must** activate alarms when resources exceeded a configurable threshold | sec.mon. 015 can be enhanced |
| 70 | SECCOM-177 | ONAP MUST support the capability of online storage of security audit logs | | | N | | | | | |
| 71 | SECCOM-178 | ONAP MUST activate security alarms automatically in following cases:<br>- when a configurable number of consecutive unsuccessful login attempts is reached<br>- when it detects the successful modification of a critical system or application file<br>- when it detects an unsuccessful attempt to gain permissions or assume the identity of another user | | | N | | | | | Alarms not in CNTT scope |
| 72 | SECCOM-179 | ONAP MUST include the following fields in the Security alarms (where applicable and technically feasible):<br>- date<br>- time<br>- service or program used for access<br>- success/failure<br>- Login ID | | | N | | | | | Alarms not in CNTT scope |
| 73 | SECCOM-180 | ONAP MUST restrict changing the criticality level of a system security alarm to users with administrative privileges | | | N | | | | | Alarms not in CNTT scope |
| 74 | SECCOM-181 | ONAP MUST monitor API invocation patterns to detect anomalous access patterns that may represent fraudulent access or other types of attacks, or integrate with tools that implement anomaly and abuse detection. | removed: It is not ONAP business to act as security management /monitoring system <br><br> Although ONAP has removed shouldn't CNTT require it. | | N | | | | | |
| 75 | SECCOM-182 | ONAP MUST collect, and be able to send any security events to a logging system, eg by syslog. The logging system needs to be able to generate security audit logs as required. | | | Y | N | | | | SEE comment on SECCOM-162 |
| 76 | SECCOM-183 | ONAP MUST log successful and unsuccessful access to ONAP resources, including data | | | N | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 77 | SECCOM-184 | ONAP logging system MUST support the storage of security audit logs for a configurable period of time | | | Y | N | | | PR#2081<br><br>Sec.mon.020<br><br>The platform's logging system must support the storage of security audit logs for a configurable period of time. | |
| 78 | SECCOM-184 | ONAP MUST store security events locally in case the logging system is unavailable | | | Y | N | | | PR#2081<br><br>sec.mon.021<br><br>The platform must store security events locally if the external logging system is unavailable and shall attempt to send these to the logging system when communications are re-established. | |
| 79 | SECCOM-185 | ONAP MUST send security events to a logging system from initialization | | | Y | N | | | PR#2081<br><br>Sec.mon.018<br><br>The platform, starting from initialization, must collect and analyze logs to identify security events, and store these events in an external system. | |
| 80 | SECCOM-186 | ONAP MUST be implemented so that it is not vulnerable to OWASP Top 10 web application security risks | | | Y | Y | Sec.std.004 | The Cloud Operator, Platform and Workloads **should** ensure that their code is not vulnerable to the OWASP Top Ten Security Risks htt ps://owasp.org /www-project-top-ten/. | | Should in CNTT |
| 81 | SECCOM-187 | ONAP MUST protect against non-volumetric denial of service attacks | | | Y | Y | | | | |
| 82 | SECCOM-188 | ONAP MUST be capable of automatically synchronizing the system clock daily with the Operator's trusted time source, to assure accurate time reporting in log files. It is recommended that Coordinated Universal Time (UTC) be used where possible, so as to eliminate ambiguity owing to daylight savings time and time zone differences. | | | Y | Y | | | | |
| 83 | SECCOM-189 | ONAP MUST have the capability to securely transmit the security logs and security events to a remote system before they are purged from the system | removed: the contents is covered in other requirements | | | | | | | |
| 84 | SECCOM-190 | ONAP SHOULD provide the capability of maintaining the integrity of its static files using a cryptographic method | removed, because operating system is not part of ONAP, and thus the ONAP user can monitor file integrity if he wants | | | | | | | |
| 85 | SECCOM-191 | ONAP MUST log automated remote activities performed with elevated privileges | removed: the other logging requirements have sufficient coverage | | | | | | | |
| 86 | SECCOM-192 | ONAP MUST provide the capability to restrict read and write access to data handled by ONAP | | | Y | Y | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control). | | |
| 87 | SECCOM-193 | ONAP MUST encrypt data in transit and protect its integrity | | | Y | Y | sec.sys.003 | The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic. | | |

| 88 | SECCOM-194 | ONAP MUST provide the capability to encrypt data on non-volatile memory.<br><br>Non-volatile memory is storage that is capable of retaining data without electrical power, e.g. Complementary metal-oxide-semiconductor (CMOS) or hard drives. | Modification in blue | | Y | Y | sec.gen.010 | The Cloud Infrastructure **must** support encrypted storage, for example, block, object and file storage, with access to encryption keys restricted based on a need to know (Controlled Access Based on the Need to Know). | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 89 | SECCOM-195 | ONAP SHOULD disable the paging of the data requiring encryption, if possible, where the encryption of non-transient data is required on a device for which the operating system performs paging to virtual memory. If not possible to disable the paging of the data requiring encryption, the virtual memory should be encrypted. | removed: not relevant for ONAP, this is on OS level | | | | | | | |
| 90 | SECCOM-196 | ONAP MUST use NIST and industry standard cryptographic algorithms and standard modes of operations when implementing cryptography. | This requirement is removed, because it is covered by CII badging section "use basic, good cryptographic practices"<br><br>Although ONAP has removed shouldn't CNTT require it. | | Y | N | | | To be added for recommendations<br><br>The platform should suppport the standard cryptographic algorithms recommended by NIST and ETSI GS NFV-SEC 012 | |
| 91 | SECCOM-197 | ONAP MUST NOT use compromised encryption algorithms. For example, SHA, DSS, MD5, SHA-1 and Skipjack algorithms. Acceptable algorithms can be found in the NIST FIPS publications (https://csrc.nist.gov/publications/fips) and in the NIST Special Publications (https://csrc.nist.gov/publications/sp). | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | | Y | N | | | | |
| 92 | SECCOM-198 | ONAP MUST use, whenever possible, standard implementations of security applications, protocols, and formats, e.g., S/MIME, TLS, SSH, IPSec, X.509 digital certificates for cryptographic implementations. These implementations must be purchased from reputable vendors or obtained from reputable open source communities and must not be developed in-house. | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | | Y | N | | | | |
| 93 | SECCOM-199 | ONAP MUST provide the ability to migrate to newer versions of cryptographic algorithms and protocols with minimal impact. | Same as #91<br><br>Software migration covered | | N | N | | | | |
| 94 | SECCOM-200 | ONAP MUST support digital certificates that comply with X.509 standards. | | | Y | N | | | PR#2081<br><br>sec.sys.017<br><br>The platform must provide the capability of using digital certificates that comply with X.509 standards and issued from a trusted Certification Authority | |
| 95 | SECCOM-201 | ONAP MUST NOT use keys generated or derived from predictable functions or values, e.g., values considered predictable include user identity information, time of day, stored/transmitted data. | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | | N | | | | | |
| 96 | SECCOM-202 | ONAP MUST provide the capability of using X.509 certificates issued by an external Certificate Authority. | appears to be duplicate of SECCOM-215 | | Y | N | | | common with requirement sec.sys.017<br><br>about X.509 | |
| 97 | SECCOM-203 | ONAP MUST be capable of protecting the confidentiality and integrity of data at rest and in transit from unauthorized access and modification. | removed: the contents is covered by other requirements<br><br>Although ONAP has removed shouldn't CNTT require it. | | Y | Y | sec.ci.001 | The Platform **must** support Confidentiality and Integrity of data at rest and in transit. | | |
| 98 | SECCOM-204 | ONAP **MUST** support the automated certificate management protocol CMPv2. Also Simple Certificate Enrollment Protocol (SCEP) or Automated Certificate Management Environment (ACME) **SHOULD** be supported. | There are 3 SECCOM-204 requirements<br><br>This is new | | N | | | | | |
| 99 | SECCOM-204 | ONAP SHOULD support installing certificates into each of its components, for example as a PKCS #12 file. | | | N | | | | | |
| 100 | SECCOM-204 | AAF MUST support installation of certificates using CMPv2, for ONAP external mTLS communication. | AAF: Authentication & Authorization Framework | | N | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 101 | SECCOM-205 | ONAP SHOULD provide the capability to integrate with an external encryption service. | | | | | | | |
| 102 | SECCOM-206 | ONAP MUST use symmetric keys of at least 112 bits in length. | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | Y for RA1 | | | | | Add to RA1 requirements |
| 103 | SECCOM-207 | ONAP MUST use asymmetric keys of at least 2048 bits in length. | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | Y for RA1 | | | | | Add to RA1 requirements |
| 104 | SECCOM-208 | ONAP MUST provide the capability to configure encryption algorithms or devices so that they comply with the laws of the jurisdiction in which there are plans to use data encryption. | Out of CNTT scope at the moment | N | | | | | |
| 105 | SECCOM-209 | ONAP MUST provide the capability of allowing certificate renewal. | There are 2 SECCOM-209 requirements | Y | N | | | PR#2081<br><br>sec.sys.018<br><br>The paltform must provide the capability of allowing certificate renewal and revocation. | Add new requirement about certificates management |
| 106 | SECCOM-209 | ONAP MUST provide the capability of allowing certificate revocation. | | Y | N | | | | Add new requirement about certificates management |
| 107 | SECCOM-210 | ONAP MUST provide the capability of testing the validity of a digital certificate by validating the CA signature on the certificate. | | Y | N | | | PR#2081<br><br>sec.sys.019<br><br>The platform must provide the capability of testing the validity of a digital certificate (CA signature, validity period, non revocation, identity). | Add new requirement about certificate validity testing |
| 108 | SECCOM-211 | ONAP MUST provide the capability of testing the validity of a digital certificate by validating the date the certificate is being used is within the validity period for the certificate. | | Y | N | | | | Add new requirement about certificate validity testing |
| 109 | SECCOM-212 | ONAP MUST provide the capability of testing the validity of a digital certificate by checking that the certificate has not been revoked. | | Y | N | | | | Add new requirement about certificate validity testing |
| 110 | SECCOM-213 | ONAP MUST provide the capability of testing the validity of a digital certificate by recognizing the identity represented by the certificate "Subject" field. | | Y | N | | | | |
| 111 | SECCOM-214 | ONAP MUST support HTTP/S using TLS v1.2 or higher with strong cryptographic ciphers. | ONAP has removed this reqt. Made it is part of badging requirement<br><br>Although ONAP has removed shouldn't CNTT require it. | N | | | | | |
| 112 | SECCOM-215 | ONAP MUST support the use of X.509 certificates issued from any Certificate Authority (CA) that is compliant with RFC5280. | | Y | N | | | see requirement<br><br>sec.sys.017<br><br>about X.509 | |