RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CENTRE NATIONAL D'ÉTUDES SPATIALES

Direction Centrale de la Sécurité
CYBER

Ref. : DCS/CYBER-20
Date : 7/9/2026
Edition : 1, Révision : 0

Checklist CNES

Prepared by Yogosha with support from CNES

Classification:	**Non sensible**
Keywords :	Cybersecurity, space, checklist
Authors:	Yogosha
Summary :	This document presents a list of security tests as an annex to CNES' Orbital System Cyb Neither Yogosha nor CNES provides any guarantee regarding the completeness or safet This document is provided solely as an appendix to the guide, for informational purposes

CATEGORY	DESCRIPTION	SUBCATEGORY	IMPLEMENTATION GOAL
Physical	Traditional physical security controls for a physical location, such as badge control, fire suppression, guards/gates/guns with proper surveillance.	Badging and Doors	Badging in and out with pin is required.
		Fire Suppression	Non-water (ex. nitrogen) fire suppression present in all critical areas.
		Gates/Guards	Perimeter fence present with 24/7 guards performing digital scanning of badges (in-lieu of digital, guards physically touch badges for inspection).
		Logging	Visitor badging for in and out required.
		Mission Security Personnel	All buildings housing critical components have 24/7 guards on duty.
		Infrastructure Diversity	All critical components have geographically dispersed (300 miles) redundancies.
		Surveillance	24/7 monitoring of video surveillance performed for all critical areas.
		Hardware Addition	Preventing physical connection (i.e. USB) and addition of hardware into the environment. Physically disable input ports that are not required.
Perimeter	Ground infrastructure has proper firewall configurations, data loss prevention, and security zones for external interactions (i.e., DMZ).	Virtual Private Network (VPN)/Remote Access	VPN, multi-factor authentication, and host verification required for access to internal system resources.
		Data Loss Prevention (DLP)	DLP policy/solution is secure and efficient.
		Demilitarized Zones (DMZs)/Securiy Zones	Services hosted for external consumption are properly protected by DMZ/security zoning AND proper limitations placed on internal network access and authentication.
		Firewall	Firewalls are configured with highly refined rulesets AND firewall configurations are routinely verified
Computer Network Defense and Incident Response	Robust architecture is established with threat hunting, intrusion detection/prevention, targeted sensor placement with TAPs and SIEMs. Security operations center functions with documented procedures and policies to detect, respond, and recover.	Forensics	Has dedicated forensics capability and personnel.
		Hunting	Personnel are trained and tasked to continuously monitor logs/traffic.
		Threat Intelligence	Collaborates with threat intelligence sources both internal and external to the organization and integrates into tools where appropriate
		IDS/IPS	IDS/IPS has insight to all critical areas of network AND staff is in place to monitor alerts 24/7.

		Incident Response Policy/Procedures	Has fully documents IR procedures. AND performs self-assessments via tabletop exercies.
		Sensors	Sensors are deployed in-line to monitor critical data flows OR sensors are place at aggregation points.
		Security Information & Event Manager (SIEM)	SIEM is present in and customized alerts are configured. AND performs 24/7 monitoring of events (on-site or remote alerting).
		Security Operations Center (SOC)	Has a local dedicated SOC with insight into all the necessary critical data flows.
		Test Access Points (TAPs)	Full deployment of TAPs in-line of all critical data flows OR TAPs are deployed in an aggregation style deployment where all critical data flows are captured.
Network	**Employment of least-trust principles with protection such as access control lists, segmentation, port security, and communication authentication.**	Reverse Proxy	Reverse Proxy installed with high availability configured along with 100% coverage on all web services.
		Access Control Lists (ACLs)	Tailored ACLs with near complete system coverage (this ties into segmentation as well).
		Authentication	Central authentication used by default (RADIUS/TACACS) with local as backup for network devices.
		Configuration/Change Management (CM)	Device configurations automatically backed up on every configuration change.
		Device Hardening	No Telnet or HTTP enabled, secure hash algorithms are used, no cisco smart install. AND Unused ports are disabled (i.e. shutdown) and in a suspended VLAN.
		Diversification of Network Paths	Fault tolerant pathways established on network Core, Distribution, and Access.
		Documentation/Diagrams	Documentation/diagrams represent the current existing configurations. AND Documentation/diagrams are part of the change process (centrally managed).
		Firewall (internal network boundaries)	Firewalls are configured with highly refined rulesets AND firewall configurations are routinely verified.
		Logging (on devices and ACLs)	Tailored logging is performed and is stored in a common central location.
		Network Access Control (NAC) - Device Authorization	Complete 100% coverage of NAC.
		Network Operations Center (NOC)	Full time NOC operated 24/7.

		Network Time Protocol (NTP)	Utilizing NTP4 consistently on all network devices.
		Port Security	Utilizing stick MACs with 3 or less reservations per port for all ports.
		Segmentation	Micro segmentation (separation of duties in network segmentation form) exists AND proper VLAN'ing with unique VLAN IDs is followed in the entire environment.
		Simple Network Management Protocol (SNMP)	Uses SNMPv3 with proper configuration (auth, server, alert settings).
		Trunking	Trunking specific VLANs while utilizing a default trunk VLAN.
		Remote Management Access	Utilizes jump boxes to manage network devices vice providing direct connection access.
		Web Proxy	Web proxy is installed with automatic configuration on hosts. AND Web proxy provides coverage on HTTP & HTTPS.
		Wireless (Could play in with Security zones really only practical for Guest)	No wireless networks in mission operations environment OR wireless networks utilize 802.1x authentication with WPA2 OR wireless networks feature Active Directory integration with WPA2 Enterprise and device level authentication
Endpoint	**Hardening of endpoint devices such as two-factor authentication, host-based intrusion detection/protection, anti-virus/malware, patching and vulnerability scanning.**	**Application Whitelisting**	Application whitelist exists and is properly used.
		Auditing	Security audits of logs are part of the security plan/policies AND security audits are efficient and executed as planned.
		Authentication	Utilizes multifactor authentication for endpoints
		Anti-virus (AV)/Anti-malware(AM)	Anti-virus or Anti-Malware are deployed, and procedures exist to keep efficient and up to date.
		Backups	Standards, solutions, and procedures for system's backups are implemented securely and efficiently AND the process and data are routinely tested and verifie
		Configuration Management (CM)/Baseline	CM/baseline standards/solution are properly implemented and efficient.
		Device Separation of Duties	Standards for permissions on device services and features are properly applied.
		Data Loss Prevention (DLP)	Data loss protection (DLP) standards/solution are properly configured and efficient.

		File Integrity	A solution for file integrity checking is used efficiently (keywords, sensitive files, etc. are identified).
		Firewall (all interfaces)	Host-based firewalls are properly configured and routinely verified.
		Hardening	Security hardening standards are implemented and routinely verified as exceeding 80%.
		Host-based Intrusion Detection System(HIDS)/Host-based Intrusion Prevention System (HIPS)	HIDS/HIPS are configured, updated, and routinely verified
		Logging	The logging process/solution is central, efficient, and reviewed frequently.
		Memory Protection	Memory protection solution is efficiently used and properly configured.
		Patch Management	Patch management program/standards is efficient, up-to-date, and properly configured for all software (OS/apps).
		Permissions	Documented application or procedure for permissions on files, directories, applications, or accounts/groups are applied correctly.
		Remote Access	Policies for remote access to systems are properly implemented using secure communication protocols.
		Service Configuration	Documented application or procedures for services' security configuration are properly implemented.
		User Least Privilege	Individual users separated by roles AND users have to reauthenticate for all elevated privileges.
		Vulnerability Scanning	A vulnerability assessment process exists where tuned scan profiles are used for all systems AND administrative credentials are used more than 90% of scans.
Ground Sofware	**Utilization of software assurance methods for all ground system software. Procedures and tools are available to prevent CWEs and eliminate CVEs as well as tracking software bill of materials. Dynamic analysis in space-centric cyber test beds is performed.**	Configuration Management (CM)/Build Environment	Stringent source code control with strong authentication (e.g., multi-factor) on software commits. Build system needs to be
		Secure Coding Standards	Secure coding standards identified in policy AND Standards are enforced during implementation (e.g., violation alerts in IDE, manual code review, etc.).
		Common Weakness Enumeration (CWE) Prevention	prioritization. This establishes wich weaknesses will have the highest impact on the spacecraft given how the software
		Documentation/Diagrams (deployed location, I/O, data types, etc)	Maintains high-level documentation of software architecture with data flows defined. AND Maintains lower-level diagrams of input/output modules with data types handled by each.
		Dynamic Testing	Performs continuous dynamic testing throughout application development, operations, and maintenance.

		Origin Analysis	Maintains a software bill of material. AND tracks all associated vulnerability information for the components. AND Regularly updates vulnerable third-party components.
		Static Code Analysis	Performs static analysis scans with a complimentary combination of tools AND has a defined process for prioritization/remediation of security related findings.
		Threat Modeling	Adheres to an exhaustive formal software threat modeling process following an established framework (or custom developed equivalent).
		Web Application Firewall (WAF)	Has a centrally deployed WAF. AND Has a process defined and implemented for configuring WAF rulesets based on application context. AND Has designated personnel with
Data	**Data-at-rest and data-in-transit encryption is utilized, TEMPEST is deployed, Operations Security (OPSEC) is practiced, permissions and access control are applied to all sensitive data**	Encryption (DAR, DIT, transport, etc)	Ensure's full disk encryption on all critical assets and for data in transit.
		Leakage	external access to sensitive documentation. AND Provides documented guidance on security culture to personnel (e.g. strong privacy controls for social media). AND Performs routine evaluations of digital footprint (public facing websites, google
		OSINT	accessible and train authorized individuals to ensure that publicly accessible information does not contain nonpublic information. Review all proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included. Educate user community on reducing OSINT footprint to limit information that can be
		Tempest	Shielding sensitive equipment from emanating electromagnetic radiation (EMR) that may carry sensitive/classified information. This is to prevent it from being intercepted by outside entities
		Permissions/Access (sensitive)	No ITAR/SBU/CUI/Sensitive/Classified data exposed and accessible with people who have no need to know. File servers/Web server's security implemented

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
Physical	Fire Suppression	PHY-001	Fire protection of buildings	Test the presence of fire extinguisher in the buildings involved in GROUND activities	
Physical	Fire Suppression	PHY-002	Fire protection of IT assets	Test the presence of fire extinguisher and A/C in the IT rooms which host GROUND activities assets	
Physical	Gates/Guards	PHY-003	Site protection	Test that all the entrances of the geographic area, which host the GROUND buildings, are protected by gates and guards (24/7). Test how they inspect the badge (physical touch, UV, digital validation, ...).	
Physical	Mission Security Personnel	PHY-004	Building protection	Test if access to buildings involved in GROUND critical activities are under guards surveillance (24/7).	
Physical	Badging and Doors	PHY-005	Badge access enforcement	Ensure that all access to geographic area, buildings and rooms are protected by gates/doors and require badge validation. Test if they can be bypassed (for example jump over a gate, two people passing with the same badge, ...).	
Physical	Surveillance	PHY-006	Camera	Test if all the critical areas are under camera sight.	
Physical	Surveillance	PHY-007	Doors	Test if attempts to bypass doors (jump, force, two people entering with the same badge, ...) lead to an alert.	
Physical	Surveillance	PHY-008	Alarms	Test for the presence of alarm systems : entrance, window openning detection, ...	
Physical	Logging	PHY-009	Visitor traceability	Test for the traceability capabilities of the visitors : ID check, sign-in sheet, mandaory badge, accompanying person to pick them up at reception, ...	
Physical	Hardware Addition	PHY-010	Employee and visitors risky equipment	Test that guards check for risky hardware to be introduced in the area and the buildings : USB keys, radio antenna, personnal laptop, ...	T1200 - Hardware Additions T1091 - Replication Through Removable Media T1052 - Exfiltration Over Physical Medium T1052.001 - Exfiltration Over Physical Medium: Exfiltration over USB
Physical	Hardware Addition	PHY-011	Hardware physical protection	Test if senstive workstations, and IT assets not locked in dedicated rooms, have disabled USB ports to prevent external hardware connection	T1200 - Hardware Additions T1091 - Replication Through Removable Media T1052 - Exfiltration Over Physical Medium T1052.001 - Exfiltration Over Physical Medium: Exfiltration over USB
Physical	Hardware Addition	PHY-012	Network endpoint protection	Test for unprotected physical access to network such as cables in false ceilings or floors, RJ45 cable connected to outdoor equipment (camera, WiFi hotspot), WiFi reachable from outdoor, ...	
Physical	Infrastructure Diversity	PHY-013	Redundancy	Ensure that all critical IT assets are redunded with a sufficient physical distance (250 km).	

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
Perimeter	Firewall	PER-001	Network isolation	Test if default filtering policy for inbound and outbound communication, from the network to uncontrolled networks (Internet, partners, ...), is set to DENY.	
Perimeter	Firewall	PER-002	Network flows minimization	Test if only necessary communications are allowed between the network and uncontrolled networks (Internet, partners, ...). In particular, forbidden ports must be denied for inbound and outbound communication to avoid on-way data exfiltration.	T1133 - External Remote Services
Perimeter	Data Loss Prevention (DLP)	PER-003	Outbound traffic limitation	Test if significant transfer rate from the network to uncontrolled networks (Internet, partners) triggers communication interruption to prevent massive data exfiltration	
Perimeter	Data Loss Prevention (DLP)	PER-004	Outbound protocol limitation	Test if opened ports can be diverted to use alternative protocols to those they are dedicated to (HTTPS on port 53, FTP on port 443, ...)	
Perimeter	Data Loss Prevention (DLP)	PER-005	Protocol encapsulation	Test if protocol encapsulation is possible : HTTP over DNS, ...	
Perimeter	Data Loss Prevention (DLP)	PER-006	External proxy	Test if outbound Web browsing is constrained to pass through a proxy. Test if protocol introspection is in place (HTTPS decryption on the fly) and ensure that it fit with confidentiality requirements.	T1090.002 - Proxy: External Proxy
Perimeter	Data Loss Prevention (DLP)	PER-007	Web filtering	Test if a filtering point (firewall or proxy) prevent to join bad reputation assets on the Web. Web browsing should be allowed on a whitelist approach.	T1102.001 - Web Service: Dead Drop Resolver T1204.001 - User Execution: Malicious Link T1568.002 - Dynamic Resolution: Domain Generation Algorithms T1189 - Drive-by Compromise T1566 - Phishing T1566.001 - Phishing: Spearphishing Attachment T1566.002 - Phishing: Spearphishing Link T1566.003 - Phishing: Spearphishing via Service
Perimeter	Demilitarized Zones (DMZs)/Securiy Zones	PER-008	DMZ	Test if services exposed to external parties are placed on a dedicated firewall interface with enforced Layer 3 filtering.	
Perimeter	Demilitarized Zones (DMZs)/Securiy Zones	PER-009	Stateful filtering	Test if DMZ rules forbid its member to initiate connection to other networks (Internet, partners, Lan, ...) except for identified needs (DNS, updates, ...). Most of the time, stateful filtering is necessary to allow assets to respond to communication initiated from other networks.	
Perimeter	Virtual Private Network (VPN)/Remote Access	PER-010	Remote access	Test if remote access to the network, for employees, is only permitted to users with explicit needs, through secure protocols (IP Sec, ...) and with MFA.	https://cyber.gouv.fr/publications/la-tele-assistance-securisee
Perimeter	Virtual Private Network (VPN)/Remote Access	PER-011	Remote assistance	Test if remote assistance is only granted to identified third party, for a limited timeslot, through secure protocols and tools, with MFA, with logging and ability to observe the actions performed.	https://cyber.gouv.fr/publications/la-tele-assistance-securisee

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
CND	Security Information & Event Manager (SIEM)	CND-001	TC disruption detection	Evaluate the capabilities (preventive and palliative), of each actor in the execution chain, to detect failure, or bad performance, in TC (Order, Ack and Result packets), at rest or in transit. Evaluate the strength of the mechanism used (QoS, alert mechanism, ...).	
CND	Security Information & Event Manager (SIEM)	CND-002	TC alteration detection	Evaluate the capabilities (preventive and palliative), of each actor in the execution chain, to detect an alteration in TC (Order, Ack and Result packets), at rest or in transit. Evaluate the strength of the mechanism used (cryptographic signature, checksum, ...).	
CND	Security Information & Event Manager (SIEM)	CND-003	Rogue TC detection	Evaluate the capabilities (preventive and palliative), of each actor in the execution chain, to detect and recognize a rogue TC (Order, Ack and Result packets), at rest or in transit. Evaluate the strength of the mechanism used (cryptographic signature, checksum, ...).	
CND	Security Information & Event Manager (SIEM)	CND-004	TC exposure detection	Evaluate the capabilities (preventive and palliative), of each actor in the execution chain, to prevent and detect illegitimate access to TC (Order, Ack and Result packets), at rest or in transit. Evaluate the strength of the mechanism used (encryption, network segmentation, ...).	
CND	IDS/IPS	CND-005	Untrusted network client	Evaluate the capabilities of the network to detect and alert when an untrusted endpoint is connected to the network.	
CND	IDS/IPS	CND-006	Protocol spoofing detection	Evaluate the capabilities of the network to detect low-level protocol poisonning such as ARP spoofing, DHCP spoofing, DNS spoofing ICMP redirect, LLMNR impersonation, ...	
CND	IDS/IPS	CND-007	DLP detection	Test if unauthorized protocols (used through authorized ports), and/or suspicious network usage rate, raises an alert	
CND	NIDS/IPS	CND-008	Active Scanning (T1595)	Monitor perimeter firewalls and NIDS/IPS for external scanning activity targeting the organization. Use threat intelligence feeds for known scanner IPs.	
CND	NIDS/IPS	CND-009	Scanning IP Blocks (T1595.001)	Test detection of network/system scanning tools (e.g., Nmap, Nessus). Monitor logs (firewall, IDS/IPS, host) for scanning patterns related to T1595.001. Verify asset inventory accuracy.	
CND	NIDS/IPS	CND-010	Remote System Discovery (T1018)	Monitor internal network scanning (e.g., ping sweeps, port scans). Implement host isolation for suspicious endpoints. Use network segmentation.	
CND	File System	CND-011	System Network Connections Discovery (T1049)	Monitor execution of commands like `netstat`, `ss`, `ipconfig`, `ifconfig`. Correlate network connection discovery with other suspicious activities.	
CND	File System	CND-012	Process Discovery (T1057)	Monitor execution of commands like `tasklist`, `ps`. Baseline normal process activity and alert on deviations. Use EDR for enhanced process monitoring.	
CND	File System	CND-013	Indicator Removal: Clear Windows Event Logs (T1070.00:	Review system configurations, logs, and security tool alerts relevant to T1070.001 (Indicator Removal: Clear Windows Event Logs). Conduct targeted tests simulating this technique in a controlled environment to verify detection and prevention capabilities. Consult MITRE ATT&CK documentation for specific procedure examples.	

CND	File System	CND-014	Indicator Removal: File Deletion (T1070.004)	Review system configurations, logs, and security tool alerts relevant to T1070.004 (Indicator Removal: File Deletion). Conduct targeted tests simulating this technique in a controlled environment to verify detection and prevention capabilities. Consult MITRE ATT&CK documentation for specific procedure examples.
CND	File System	CND-015	Application Layer Protocol (T1071)	Monitor network traffic for unusual usage of standard protocols (HTTP/S, FTP, DNS). Baseline normal application traffic. Use protocol analysis and application-aware firewalls.
CND	SIEM	CND-016	Indicator Removal (T1070)	Enable and secure audit logs. Implement log forwarding to a central SIEM. Monitor for attempts to clear logs (e.g., `wevtutil cl`) or tamper with timestamps. Use FIM for critical log files.
CND	File System	CND-017	Ingress Tool Transfer (T1105)	Monitor downloads from external sources. Scan transferred files for malware. Use web proxies and email gateways with content filtering. Restrict execution from download directories.
CND	File System	CND-018	Data Encoding (T1132)	Monitor for encoded data within network traffic or files where it is not expected. Use tools capable of decoding standard encodings (Base64, etc.) for inspection.
CND	File System	CND-019	Archive Collected Data (T1560)	Monitor for the use of archiving utilities (zip, 7z, tar) on large volumes of data or sensitive file types. Alert on unusual file compression activity.
CND	File System	CND-020	Non-Standard Port (T1571)	Monitor network traffic for protocols running on non-standard ports (e.g., RDP on port 80). Use application-aware firewalls to enforce standard port usage.
CND	DLP	CND-021	Exfiltration Over Web Service (T1567)	Monitor uploads to cloud storage and other web services. Implement DLP policies to detect sensitive data in outbound traffic. Restrict access to unauthorized file sharing sites.
CND	DLP	CND-022	Encrypted Channel (T1573)	Monitor for initiation of encrypted sessions to unknown or suspicious external hosts. Use TLS/SSL inspection where possible. Analyze metadata of encrypted traffic (e.g., JA3/JA3S hashes).

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
Network	Access Control Lists (ACLs)	NET-001	Disrupt TC Order	Try to prevent/block/disturb/slow TC order (from GROUND to SAT), during transmission between each component of the execution chain, in a way that prevent them to properly work.	
Network	Access Control Lists (ACLs)	NET-002	Disrupt TC ACK	Try to prevent/block/disturb/slow TC Ack (from SAT to GROUND), during transmission between each component of the communication chain, in a way that prevent them to properly work.	
Network	Access Control Lists (ACLs)	NET-003	Disrupt TC Result	Try to prevent/block/disturb/slow TC Result (from SAT to GROUND), during transmission between each component of the communication chain, in a way that prevent them to properly work.	
Network	Access Control Lists (ACLs)	NET-004	Tamper TC Order	Try to alter TC order, during transmission between each component of the execution chain, to execute another function.	
Network	Access Control Lists (ACLs)	NET-005	Craft TC Order	Try to craft or replay TC Order transmission packets between each component in the execution chain.	
Network	Access Control Lists (ACLs)	NET-006	Tamper TC ACK	Try to alter TC Ack (from SAT to GROUND), during transmission between each component of the communication chain, to change the legitimate state (OK instead of KO, KO instead of OK).	
Network	Access Control Lists (ACLs)	NET-007	Craft TC ACK	Try to craft a fake TC Ack packet (from SAT to GROUND), during transmission between each component of the communication chain, to change the legitimate state (OK instead of KO, KO instead of OK).	
Network	Access Control Lists (ACLs)	NET-008	Disclose TC Order	Try to access to TC order content (from GROUND to SAT), during transmission between each component of the execution chain.	
Network	Access Control Lists (ACLs)	NET-009	Disclose TC ACK	Try to access to TC Ack content (from SAT to GROUND), during transmission between each component of the execution chain.	
Network	Access Control Lists (ACLs)	NET-010	Disclose TC Result	Try to access to TC Result content (from SAT to GROUND), during transmission between each component of the execution chain.	
Network	Segmentation	NET-011	Network surface reduction	Test if only necessary network services are reachable from a subnet to another. Evaluate the strength of the mechanism used (VLan filtering, micro-segmentation, ...)	
Network	Network Access Control (NAC) - Device Authorization	NET-012	Rogue endpoint prevention	Test if the network prevent untrusted endpoints to connect. Evaluate the strength of the mechanism used (802.1X, MAC whitelist, ...)	
Network	Segmentation	NET-013	Local subnet enumeration	Test if the network prevent an endpoint to discover its immediate subnet. Evaluate the strenght of the mechanism used (private VLan, local firewall, ...)	
Network	Device Hardening	NET-014	Protocols security	Test for the usage or presence of unencrypted and/or unauthenticated network protocols (such as telnet, tftp, mqtt, ...)	
Network	Segmentation	NET-015	Interface isolation	Test if remote management services are reachable on the production network interfaces (instead of being restricted to an administration network interface only)	
Network	Configuration/Change Management (CM)	NET-016	Default configuration	Test for default credential or key material used in network protocols (certificate, password, username, ...)	
Network	Authentication	NET-017	Test for weak authentication between trusted systems.	Assess the authentication mechanisms used in trusted relationships, looking for weaknesses or misconfigurations in how systems authenticate each other. Ensure that all internal communication between mission systems is properly secured and authenticated to prevent unauthorized access.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1199/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078/
Network	Device Hardening	NET-018	Exploit Outdated or vulnerable services.	Identify publicly disclosed vulnerabilities (e.g., CVEs) for services running on open TCP ports and leverage available exploits to compromise systems or gain deeper access. Exploit known vulnerabilities in open services to gain unauthorized access, escalate privileges, or disrupt mission operations.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1588.005/
Network	Device Hardening	NET-019	Scan for open or misconfigured TCP ports.	Perform port scanning to identify open TCP ports that may be exposed to external attackers and access the current configuration Detect exposed services that could be targeted for initial access, such as unfiltered ports or legacy services.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.001/
Network	Firewall (internal network boundaries)	NET-020	Disrupt Command Uplinks	Target uplink communication channels to disrupt or block spacecraft command signals. Prevent mission operators from controlling or adjusting spacecraft operations.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1485/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1531/
Network	Firewall (internal network boundaries)	NET-021	Perform denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks.	Test the resilience of network-facing TCP services by attempting DoS or DDoS attacks. Identify vulnerabilities in network infrastructure that could be exploited to interrupt mission operations.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1498.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1498.002/

Network	Network Operations Center (NOC)	NET-022	Analyze Network Connections	Monitor outbound and inbound network connections to identify relationships between services and potential vulnerabilities. Understand the communication landscape to exploit weaknesses or misconfigurations in service dependencies.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1016/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1040/
Network	Network Operations Center (NOC)	NET-023	Monitor Network Traffic for Unencrypted Credentials	Passively capture and analyze network traffic to identify unencrypted credentials being transmitted over the network, such as plaintext usernames and passwords. Detect and mitigate insecure communication practices that could expose sensitive credentials to potential interception.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1040/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.001/
Network	Segmentation	NET-024	Identify and exploit trust relationships with third-party vendors.	Investigate trust relationships with third-party vendors, contractors, or partners that provide services or infrastructure to the MOC or Ground Control. Identify vulnerabilities in third-party services that could be leveraged to gain access to mission systems.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1199/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.002/
Network	Segmentation	NET-025	Map out internal trust relationships.	Map the trust relationships between mission systems, such as dependencies on external satellite communication systems or trust between Ground Control and remote telemetry stations. Identify weak or poorly configured trust relationships that could be exploited to gain access to internal systems.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1199/

Category	Sub-category	Check Referenc	Check Title	Check Description	Check URL (link to external page)
Endpoint	Auditing		Enumerate Users, Roles, and Processes	List all users, roles, processes, and their permissions to understand relationships between accounts and services that could be exploited for privilege escalation. Identify misconfigurations or oversights that could allow unauthorized privilege escalation or lateral movement.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1087/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1057/
Endpoint	Authentication		Backdoor Authentication Mechanisms	Modify or backdoor authentication mechanisms, such as SSH keys or login scripts, to enable reentry without detection. Maintain persistent access while minimizing the risk of detection.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1098.004/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1556.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1556.003/
Endpoint	Authentication		Check for default or easily guessable credentials.	Look for accounts that still use default credentials or are based on easily guessable combinations (e.g., root:root, Guest:guest). Ensure that accounts are protected with strong, unique passwords to prevent unauthorized access.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078.001/
Endpoint	Authentication		Test for reused passwords.	Gather a list of all the Authentification Security Control located on the infrastructure and Test accounts for passwords reuse in multiple Services that may be easy to exploit. Identify accounts that can be compromised using password reuses, simple brute-force or dictionary attacks.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1110.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1110.002/
Endpoint	Backups		Force Use of Backup Systems to Test Security Controls	Disrupt primary mission-critical functions or processes to force the MOC to transition operations to backup systems, then assess the security controls and procedures of the backup systems. Evaluate whether backup systems maintain equivalent security measures to the primary systems and identify vulnerabilities that could be exploited during the transition or while operating on the backup.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1485/
Endpoint	Configuration Management (CM)/Baseline		Create or Modify Scheduled Tasks or Cron Jobs	Identify or create scheduled tasks or cron jobs that execute malicious payloads at a certain mission-critial time. Establish the possibility of a delayed action to impact the Integrity or Availability of the System.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1053.003/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1053.005/
Endpoint	File Integrity		Test for Abusable Application Folder/Scripts, Source Code Repositories, Shared Documents, or Mission Files	Search for and identify key internal processes or critical application points that could be exploited to impact the integrity of the system. Identify locations where malicious commands or code could be introduced into the mission's regular operation, ensuring that such modifications remain persistent and execute undetected.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1562.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1574/
Endpoint	Permissions		Analyze Writable Files and Directories	Scan the local file system for writable files and directories that may allow privilege escalation through modification or exploitation. Detect insecure configurations that could allow unauthorized modification of critical files or scripts.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1068/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1546/

Endpoint	Permissions		Identify unused or inactive accounts.	Review user account management systems for inactive or unused accounts that may still be valid and provide an entry point. Detect forgotten or overlooked accounts that could be used by attackers for unauthorized access.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1589.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1078.003/
Endpoint	Permissions		Review Sudo and Sudoer Permissions	Check the sudo permissions and configuration to identify misconfigurations that could be exploited to escalate privileges. Detect weaknesses in sudo policies that could allow unauthorized command execution or privilege escalation.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1068/
Endpoint	Service Configuration		Identify Internally Exposed Services	Check for services listening on localhost to identify potential attack vectors that are internally exposed. Discover hidden services that may be vulnerable to exploitation for privilege escalation or lateral movement.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1021.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1021.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1021.003/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1021.004/
Endpoint	Vulnerability Scanning		Check for Public Exploits	Research and test public exploits for vulnerabilities in the Linux kernel or other components on the target system. Identify and exploit known vulnerabilities to gain elevated privileges.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1068/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1588.005/
Endpoint	Vulnerability Scanning		Run Privilege Escalation Recon Tools	Execute automated privilege escalation scripts such as LinPEAS or LinEnum to perform a comprehensive reconnaissance of the system, identifying potential escalation paths. Review the output for misconfigurations, sensitive data, or exploitable vulnerabilities. Systematically detect privilege escalation opportunities, such as writable Bus, SetUID Binary, Uncommon Programs or other unconvential escaltion path that could be leveraged to gain higher privileges.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1068/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1016/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1518/
Endpoint	Vulnerability Scanning		Scan for exposed administrative interfaces.	Identify network-facing administrative interfaces within the MOC or Ground Control systems that may be exposed to unauthorized users or external networks. Find accessible points of entry that could be targeted to access Sensitive Data that would help gain more knowledge about the Internal system or lead to an Initial Foothold.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.001/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/
Endpoint	Attack Simulation		Adversary-in-the-Middle	Test network segmentation. Implement ARP spoofing detection. Use DHCP snooping. Deploy TLS/SSL inspection where appropriate. Monitor for certificate warnings or anomalies.	https://attack.mitre.org/techniques/T1557/

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
Ground Software	Origin Analysis	GS-TTP-001	Test for outdated or vulnerable HTTP service or 3rd Party library.	Detect and Verify all web applications service for outdated software versions that may have known vulnerabilities. Cross-reference software component reconnaissance results with publicly available exploits that could be used to affect the confidentiality, integrity, or availability of the mission	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1588.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1588.005/
Ground Software	Secure Coding Standards	GS-TTP-002	Check for Common Web Vulnerability	Identify application parameter that could be exploited by less critical Web Vulnerability that could still prevent a risk in Edges cases Ensure that the application correctly sanitizes user input to prevent vulnerabilities such as Cross-Site Scripting (XSS), Insecure Direct Object References (IDOR), XML Injection, and Database Injection and other OWASP Top 10	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1189/
Ground Software	Secure Coding Standards	GS-TTP-003	Check for Local File Inclusion (LFI) vulnerabilities.	Search for web applications susceptible to LFI vulnerabilities, where attackers can include local files from the server to expose sensitive data or execute arbitrary code. Ensure that input validation is implemented correctly to prevent unauthorized access to local files on the server.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1059.004/
Ground Software	Secure Coding Standards	GS-TTP-004	Check for Path Traversal vulnerabilities.	Test for path traversal vulnerabilities, where attackers can manipulate file paths to read or write access files outside the intended directory. Ensure that input sanitization prevents attackers from accessing files outside the application's allowed directories.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/
Ground Software	Secure Coding Standards	GS-TTP-005	Deplete Onboard Resources	Exploit systems to drain onboard resources like power, fuel, or computing cycles. Accelerate mission resource depletion, shortening the operational lifespan.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1499/
Ground Software	Secure Coding Standards	GS-TTP-006	Exploit Software or Firmware Vulnerabilities	Identify and exploit vulnerabilities in spacecraft software or firmware to degrade mission functionality. Introduce errors or gain control over systems to disrupt mission-critical functions.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1588.005/
Ground Software	Secure Coding Standards	GS-TTP-007	Test for Remote Code Execution (RCE) vulnerabilities.	Identify web applications that allow the execution of arbitrary code or system commands via user input. Check for user input fields or file upload mechanisms that could allow attackers to execute malicious commands on the server.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1059.004/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1059.005/
Ground Software	Threat Modeling	GS-TTP-008	Examine exposed APIs or endpoints Access Control	Review Application Client-Side HTML Source code to gather APIs, Endpoints and Parameters for potential weaknesses or misconfigurations that can be exploited. Identify unprotected or poorly configured APIs that provide access to mission-critical resources.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1595.002/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1598/

Ground Software	Binary Protections	GS-TTP-009	Verify software integrity checks	Verify software integrity checks (e.g., code signing, checksums) for critical client applications. Attempt to replace a legitimate binary with a modified one and observe system behavior and logs.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1574/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1218/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1553/
Ground Software	Vulnerability Assessment	GS-TTP-010	Exploit Public-Facing Application	Perform vulnerability scanning (e.g., using Nessus, OpenVAS) against web servers and applications. Conduct penetration testing focusing on common web vulnerabilities (SQLi, XSS, RCE). Review WAF logs for blocked exploit attempts.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1190/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1203/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1505.003/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1071.001/
Ground Software	Credential Security	GS-TTP-011	Exploitation for Credential Access	Test applications for vulnerabilities that could lead to credential disclosure (e.g., hardcoded credentials, insecure storage). Use credential harvesting tools in a controlled manner to test detection capabilities.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1555/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1003/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1649/

Category	Sub-category	Check Reference	Check Title	Check Description	Check URL (link to external page)
Data	Permissions/ Access (sensitive)	GS-TTP-001	Disrupt TC Order content at rest	Try to alter TC Order, at the locations where they are stored, in a way that prevent them to properly work.	
Data	Permissions/ Access (sensitive)	GS-TTP-002	Disrupt TC Ack content at rest	Try to alter TC Ack, at the locations where they are stored, in a way that prevent them to properly work.	
Data	Permissions/ Access (sensitive)	GS-TTP-003	Disrupt TC Result content at rest	Try to alter TC Result, at the locations where they are stored, in a way that prevent them to properly work.	
Data	Permissions/ Access (sensitive)	GS-TTP-004	Tamper TC Order at rest	Try to modify TC Order, at the locations where they are stored, in a way to execute another function.	
Data	Permissions/ Access (sensitive)	GS-TTP-005	Tamper TC Ack at rest	Try to modify TC Ack, at the locations where they are stored, in a way to execute another function.	
Data	Permissions/ Access (sensitive)	GS-TTP-006	Tamper TC Result at rest	Try to modify TC Result, at the locations where they are stored, in a way to execute another function.	
Data	Permissions/ Access (sensitive)	GS-TTP-007	Craft TC Order at rest	Try to create a rogue TC order, at the location where legitimate ones are stored.	
Data	Permissions/ Access (sensitive)	GS-TTP-008	Craft TC Ack at rest	Try to create a rogue TC Ack, at the location where legitimate ones are stored.	
Data	Permissions/ Access (sensitive)	GS-TTP-009	Craft TC Result at rest	Try to create a rogue TC Result, at the location where legitimate ones are stored.	
Data	Permissions/ Access (sensitive)	GS-TTP-010	Disclose TC Order at rest	Try to access TC Order, at the locations where they are stored, to read their content.	
Data	Permissions/ Access (sensitive)	GS-TTP-011	Disclose TC at rest	Try to access TC Ack, at the locations where they are stored, to read their content.	
Data	Permissions/ Access (sensitive)	GS-TTP-012	Disclose TC at rest	Try to access TC Result, at the locations where they are stored, to read their content.	
Data	Leakage	GS-TTP-013	Manipulate Telemetry Data	Alter or manipulate telemetry data transmitted from the spacecraft to mission operators. Deceive operators into making incorrect decisions based on falsified data.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1565/
Data	Leakage	GS-TTP-014	Search Readable Files for Sensitive Information	Locate readable files containing sensitive information, such as cached credentials, service keys, or configuration files. Gather sensitive information that can be leveraged for privilege escalation or lateral movement.	https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1003/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1555/ https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-16.1/domain-enterprise/techniques/T1039/
Data	Automated Collection	GS-TTP-015	Test controls for detecting and mitigating attacker actions related to Automated Collection (T1119) within the Data layer.	Test data loss prevention (DLP) rules. Simulate automated data gathering scripts (e.g., searching for specific file types or keywords across network shares) and verify if detection/blocking occurs. Check access logs for unusual patterns of file access.	T1119 Automated Collection
Data	Cloud Storage Object Discovery	GS-TTP-016	Test controls for detecting and mitigating attacker actions related to Cloud Storage Object Discovery (T1619) within the Data layer.	If cloud storage is used, check access controls and permissions on buckets/containers. Attempt unauthorized enumeration of objects. Monitor cloud logs for suspicious API calls related to storage listing.	T1619 Cloud Storage Object Discovery
Data	Data Destruction	GS-TTP-017	Test controls for detecting and mitigating attacker actions related to Data Destruction (T1485) within the Data layer.	Test file integrity monitoring (FIM) systems. Attempt to delete or overwrite critical data files in a test environment and verify if alerts are generated. Review backup and recovery procedures.	T1485 Data Destruction

Bibliography:

https://cnes.fr/en/business/space-cybersecurity-center

https://sparta.aerospace.org/related-work/threats/ground

https://sparta.aerospace.org/related-work/did-space#