TOS access hardening checklist

For: IT managers, system engineers and security leads of a container or multipurpose terminal

Walk the checklist with the people who run the terminal operating system (TOS): its application, database and integration servers, the accounts on them, the remote paths into them and the interfaces that feed them. For each line, write who owns it, where the evidence is kept and its status. Start with the lines marked missing on the servers the terminal cannot work without.

Scope. The TOS is the software that plans and records the work of the terminal: where every container is, which crane or truck moves it next, what the gate lets in or out. This checklist covers access to it: privileged accounts, remote access by vendors and support teams, the APIs and interfaces that exchange data with it, and the logs that show who did what. The cranes and yard machines (OT) are covered by another page of this site.

Five families

• **P · Privileged accounts**: Few administrators, each with a named admin account kept apart from daily work, strong authentication, and accounts closed when people leave.

• **V · Remote vendor access**: One approved path in, opened for a stated job, named accounts with multi-factor authentication, every third-party session recorded.

• **I · APIs and interfaces**: Know every interface that reads or writes TOS data, authenticate each partner separately, let each one see only its own data.

• **L · Logging**: The security logs of the TOS servers reach a place the TOS administrators cannot erase, with the right audit settings and the same clock.

• **D · Detection**: Two open rules watch remote logons and new administrators on the TOS servers, and someone reads the alert the same day.

Status

• in place · the evidence exists, is dated and someone owns it

• partial · done for some servers, accounts or interfaces only, or the evidence is out of date

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal: _____ · system: _____ · date: _____

Item	References	Status	Owner
P1 · A list of every privileged account	33 CFR 101.650(a)(5) · AA23-278A, misconfiguration 2		
P2 · Admin accounts kept apart from daily accounts	33 CFR 101.650(a)(6) · AA23-278A, misconfiguration 2		
P3 · Multi-factor authentication for administrators	33 CFR 101.650(a)(4) · IMO Rev.4 3.5.3.2 · AA23-278A, misconfiguration 7		
P4 · No default password, lockout on repeated failures	33 CFR 101.650(a)(1)-(3) · AA23-278A, misconfiguration 1		
P5 · Accounts closed when people leave	33 CFR 101.650(a)(7) · CISA remote access guide (June 2023)		
V1 · One approved path in	33 CFR 101.650(e)(3)(iv) · CISA remote access guide (June 2023)		
V2 · Access opened for a job, closed after it	NIST SP 800-82r3 6.2.10		
V3 · Named vendor accounts with multi-factor authentication	IMO Rev.4 3.5.3.1, 3.5.3.2 · 33 CFR 101.650(a)(4)		
V4 · Every third-party session monitored	33 CFR 101.650(f)(3)		
V5 · Remote access tools inventoried and allowed by name	CISA remote access guide (June 2023)		
V6 · Vendors tell you about their vulnerabilities and incidents	33 CFR 101.650(f)(2)		
I1 · Every interface listed	OWASP API9:2023 · 33 CFR 101.650(b)(3)		
I2 · One credential per partner, never shared	OWASP API2:2023		
I3 · Each partner sees only its own data	OWASP API1:2023		
I4 · Limits on what an interface can ask	OWASP API4:2023		
I5 · Interface calls logged	33 CFR 101.650(c)(1)		
L1 · The TOS servers' security logs reach the SIEM	AA23-278A, misconfiguration 3		
L2 · The audit settings the rules need are on	Microsoft, events 4624 and 4732		
L3 · Logs the TOS administrators cannot erase	33 CFR 101.650(c)(1) · CISA remote access guide (June 2023)		
L4 · One clock, a retention period that is written	NIST SP 800-92		
L5 · IT and OT connections logged	33 CFR 101.650(h)(2)		
D1 · Alert on remote logons from outside the admin network	Microsoft 4624 · MITRE ATT&CK T1021.001		
D2 · Alert on a new local administrator	Microsoft 4732 · MITRE ATT&CK T1098		
D3 · Tested on past logs before the alert is on	PCA detection rules README		
D4 · Someone reads the alert the same day	33 CFR 101.650(g)(2)		

P · Privileged accounts

Few administrators, each with a named admin account kept apart from daily work, strong authentication, and accounts closed when people leave.

P1 · A list of every privileged account *(33 CFR 101.650(a)(5) · AA23-278A, misconfiguration 2)*

What to check: The terminal keeps a list of the accounts with administrator rights on the TOS servers, the TOS application and its database, including service accounts and vendor accounts, with the person or system behind each one.

Why: 33 CFR 101.650(a)(5) requires least privilege for administrator and other privileged accounts on IT and OT. The NSA/CISA advisory of October 2023 lists excessive account privileges among its top ten misconfigurations (improper separation of user and administrator privilege). Least privilege cannot be checked without the list.

Evidence to hold: [ ] The list of privileged accounts per server and per application, with an owner for each · [ ] The date of the last review and who signed it

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P2 · Admin accounts kept apart from daily accounts *(33 CFR 101.650(a)(6) · AA23-278A, misconfiguration 2)*

What to check: An administrator uses a separate, named admin account for administration of the TOS, and a normal account for mail and web. No one reads mail or browses the web with an account that administers the TOS.

Why: 33 CFR 101.650(a)(6) asks that users keep separate credentials on critical IT and OT systems. The NSA/CISA advisory names improper separation of user and administrator privilege as misconfiguration 2.

Evidence to hold: [ ] The list of administrators with their daily account and their admin account · [ ] The rule that forbids mail and browsing with an admin account

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P3 · Multi-factor authentication for administrators *(33 CFR 101.650(a)(4) · IMO Rev.4 3.5.3.2 · AA23-278A, misconfiguration 7)*

What to check: Every administrator logon to the TOS servers and the TOS administration console asks for a second factor. Where it cannot, the compensating control is written down.

Why: 33 CFR 101.650(a)(4) requires multi-factor authentication on password-protected IT and on remotely accessible OT, with documented compensating controls when it is not feasible. IMO Rev.4 asks for multi-factor or continuous authentication (3.5.3.2). The NSA/CISA advisory lists weak or misconfigured multi-factor methods as misconfiguration 7.

Evidence to hold: [ ] Which logons ask for a second factor, server by server · [ ] The written compensating control for each exception

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P4 · No default password, lockout on repeated failures *(33 CFR 101.650(a)(1)-(3) · AA23-278A, misconfiguration 1)*

What to check: Default passwords of the TOS, its database and its servers were changed before use. Accounts lock after repeated failed logins, and a minimum password strength is enforced.

Why: 33 CFR 101.650(a)(1) to (a)(3) require automatic lockout after repeated failed logins, default passwords changed before use, and a minimum password strength. The NSA/CISA advisory puts default configurations first in its list.

Evidence to hold: [ ] The record that default passwords were changed, per component · [ ] The lockout and password settings as read on the servers, with the date read

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P5 · Accounts closed when people leave *(33 CFR 101.650(a)(7) · CISA remote access guide (June 2023))*

What to check: When an employee, contractor or vendor engineer leaves, their accounts on the TOS and its servers are removed or disabled, and any shared secret they knew is changed.

Why: 33 CFR 101.650(a)(7) requires that user credentials are removed or revoked when a user leaves the organisation. The CISA-led remote access guide recommends auditing Active Directory for inactive and obsolete accounts.

Evidence to hold: [ ] The leaver procedure and the last three leavers with the date their accounts were closed · [ ] The list of accounts unused for a long time, and what was decided for each

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V · Remote vendor access

One approved path in, opened for a stated job, named accounts with multi-factor authentication, every third-party session recorded.

V1 · One approved path in (33 CFR 101.650(e)(3)(iv) · CISA remote access guide (June 2023))

What to check: Vendors and support teams reach the TOS servers through one approved path (a jump host, a VPN or a remote desktop gateway), never directly from the Internet. The list of approved paths is written and short.

Why: 33 CFR 101.650(e)(3)(iv) requires that no exploitable channel is directly exposed to Internet-accessible systems. The CISA-led remote access guide recommends using remote access solutions such as VPNs or virtual desktops. The first Sigma rule on this page relies on this list.

Evidence to hold: [ ] The list of approved remote access paths, with the address of each one · [ ] The result of the last check that the TOS servers are not reachable directly from the Internet

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V2 · Access opened for a job, closed after it (NIST SP 800-82r3 6.2.10)

What to check: A vendor asks before each remote session; the terminal opens access for the stated job, on the servers concerned, and closes it at the end. Standing, always-on vendor access is the exception, and written down.

Why: NIST SP 800-82 Rev. 3 asks for a process for requesting and enabling remote access, and says it should be provided only if justified and limited to what the business need requires (6.2.10).

Evidence to hold: [ ] The remote access procedure · [ ] The record of the last sessions: who, which server, why, start and end

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V3 · Named vendor accounts with multi-factor authentication (IMO Rev.4 3.5.3.1, 3.5.3.2 · 33 CFR 101.650(a)(4))

What to check: Each vendor engineer has a named account (no shared vendor login) and uses multi-factor authentication on the approved path.

Why: IMO Rev.4 asks for unique credentials for all users (3.5.3.1) and for multi-factor or continuous authentication (3.5.3.2). 33 CFR 101.650(a)(4) requires multi-factor authentication on password-protected IT.

Evidence to hold: [ ] The list of vendor accounts with the person behind each one · [ ] The second factor used on the approved path

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V4 · Every third-party session monitored (33 CFR 101.650(f)(3))

What to check: Every remote connection by a third party is recorded (who, from where, when, to which server) and someone looks at the record.

Why: 33 CFR 101.650(f)(3) requires the owner or operator to monitor and document all third-party remote connections to detect cyber incidents.

Evidence to hold: [ ] Where the session records are kept, and how long · [ ] The last review of the records, by whom

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V5 · Remote access tools inventoried and allowed by name (CISA remote access guide (June 2023))

What to check: The terminal knows which remote access and remote monitoring tools are installed on the TOS servers. Only the approved ones may run; any other one found is removed.

Why: The CISA-led remote access guide (June 2023) recommends auditing remote access software and its configuration on the network, and application controls that allowlist approved remote monitoring and management tools.

Evidence to hold: [ ] The list of approved remote access tools, per server · [ ] The result of the last search for tools that are not on the list

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

V6 · Vendors tell you about their vulnerabilities and incidents *(33 CFR 101.650(f)(2))*

What to check: The contract with each vendor that can reach the TOS says it notifies the terminal, without delay, of vulnerabilities in what it supplies and of cyber incidents that may affect the terminal.

Why: 33 CFR 101.650(f)(2) requires a process through which IT and OT vendors and service providers notify the owner or operator of vulnerabilities and reportable cyber incidents without delay.

Evidence to hold: [ ] The clause in each contract, or the letter that adds it · [ ] The contact on each side

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I · APIs and interfaces

Know every interface that reads or writes TOS data, authenticate each partner separately, let each one see only its own data.

I1 · Every interface listed (OWASP API9:2023 · 33 CFR 101.650(b)(3))

What to check: The terminal keeps a list of the APIs, EDI flows and file exchanges that read or write TOS data (gate, port community system, shipping lines, rail, customs, customer portals), with the partner, the direction and the owner.

Why: The OWASP API Security Top 10 (2023) lists improper inventory management (API9): interfaces nobody tracks stay open with old versions. 33 CFR 101.650(b)(3) requires an accurate inventory of network-connected systems.

Evidence to hold: [ ] The interface list, with the date of the last update · [ ] The interfaces switched off since the last review

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I2 · One credential per partner, never shared (OWASP API2:2023)

What to check: Each partner system authenticates with its own credential (key, certificate or account). A credential is never shared between partners and is revoked when the partner stops using the interface.

Why: Broken authentication is API2 in the OWASP API Security Top 10 (2023). One credential per partner is what lets the terminal revoke one partner without stopping the others, and know which partner made a call.

Evidence to hold: [ ] The list of credentials per partner, with their creation date · [ ] The last credential revoked, and when

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I3 · Each partner sees only its own data (OWASP API1:2023)

What to check: The interface checks, on every call, that the partner may see or change the record asked for: a trucking company sees its own bookings, a shipping line its own containers.

Why: Broken object level authorisation is API1 in the OWASP API Security Top 10 (2023): an interface that returns any record whose number is asked for leaks the whole terminal one record at a time.

Evidence to hold: [ ] The test that asks for another partner's record and is refused, with its date

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I4 · Limits on what an interface can ask (OWASP API4:2023)

What to check: Each interface has limits on calls and on the size of answers, so one partner, by mistake or not, cannot slow the TOS for everyone.

Why: Unrestricted resource consumption is API4 in the OWASP API Security Top 10 (2023).

Evidence to hold: [ ] The limits set per interface · [ ] What happens when a partner reaches them (refused, queued, alerted)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I5 · Interface calls logged (33 CFR 101.650(c)(1))

What to check: Calls to the interfaces are logged with the partner, the time, the operation and the result, and those logs go to the same protected store as the server logs.

Why: 33 CFR 101.650(c)(1) requires logs to be securely captured, stored and protected. Without call logs, the terminal cannot tell which partner read or changed a record.

Evidence to hold: [ ] A sample of the interface log, with the fields it holds · [ ] Where those logs are stored

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

L · Logging

The security logs of the TOS servers reach a place the TOS administrators cannot erase, with the right audit settings and the same clock.

L1 · The TOS servers' security logs reach the SIEM (AA23-278A, misconfiguration 3)

What to check: The Windows Security log (or the authentication log on Linux) of every TOS application, database and integration server is forwarded to the SIEM or the central log store. A search for the last day returns events from each one.

Why: The NSA/CISA advisory of October 2023 names insufficient internal network monitoring as misconfiguration 3. A detection rule fires only on logs that arrive.

Evidence to hold: [ ] The list of TOS servers with the date their logs were last seen in the SIEM

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

L2 · The audit settings the rules need are on (Microsoft, events 4624 and 4732)

What to check: On the TOS servers, the audit policy records successful logons and security group changes. It was read on the servers (for example with auditpol), not assumed.

Why: Microsoft documents a successful logon as event 4624 and a member added to a local security group as event 4732; each is written only if the matching audit policy is enabled. The two Sigma rules on this page rely on them.

Evidence to hold: [ ] The audit policy as read on one server of each type, with the date read

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

L3 · Logs the TOS administrators cannot erase (33 CFR 101.650(c)(1) · CISA remote access guide (June 2023))

What to check: The log store is outside the reach of the TOS administrators and of the remote access tools: they cannot delete or change its content. Only a few named people can read it.

Why: 33 CFR 101.650(c)(1) requires logs to be securely captured, stored and protected so that only privileged users can reach them. The CISA-led remote access guide recommends keeping direct access to log servers, and the ability to delete or alter logs, out of reach of remote management tools.

Evidence to hold: [ ] Who can read and who can delete in the log store

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

L4 · One clock, a retention period that is written (NIST SP 800-92)

What to check: All TOS servers and the log store take their time from the same source, and the terminal has written how long it keeps logs and why.

Why: NIST SP 800-92 explains that log entries from different hosts can only be correlated when clocks are synchronised, and asks organisations to set log retention in their policy. We give no number: the period depends on your rules and on what an investigation needs.

Evidence to hold: [ ] The time source of each server · [ ] The written retention period

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

L5 · IT and OT connections logged (33 CFR 101.650(h)(2))

What to check: Where the TOS exchanges data with OT (cranes, yard equipment, gate automation), those connections are logged and watched.

Why: 33 CFR 101.650(h)(2) requires that all connections between IT and OT are logged and monitored for suspicious activity, unauthorised access and cyber incidents.

Evidence to hold: [ ] The list of IT-OT connections and where their logs are kept

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D · Detection

Two open rules watch remote logons and new administrators on the TOS servers, and someone reads the alert the same day.

D1 · Alert on remote logons from outside the admin network *(Microsoft 4624 · MITRE ATT&CK T1021.001)*

What to check: The rule « Remote Desktop Logon to a TOS Server From Outside the Admin Network » runs in the SIEM, with your server names and your approved paths (V1) in place of the example values.

Why: A successful remote desktop logon is event 4624 with logon type 10 (Microsoft). Remote desktop is a common way for an intruder to move between servers (MITRE ATT&CK T1021.001). A session from outside the approved paths deserves a look the same day.

Evidence to hold: [ ] The converted search in the SIEM, with the date it went live · [ ] The filter of approved paths, matching V1

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D2 · Alert on a new local administrator *(Microsoft 4732 · MITRE ATT&CK T1098)*

What to check: The rule « Account Added to the Local Administrators Group of a TOS Server » runs in the SIEM, with your server names in place of the example values.

Why: Microsoft records an account added to a local security group as event 4732. Adding an account to a privileged group is a known way to keep access (MITRE ATT&CK T1098, account manipulation).

Evidence to hold: [ ] The converted search in the SIEM, with the date it went live

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D3 · Tested on past logs before the alert is on *(PCA detection rules README)*

What to check: Each rule was first run on recent past logs. Each hit was explained: a real question, or a missing line in the filter that was then added.

Why: A rule that fires on every approved session is soon ignored. Running it backwards first makes the first live alert worth reading.

Evidence to hold: [ ] The result of the backward run and the filter lines added after it

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D4 · Someone reads the alert the same day *(33 CFR 101.650(g)(2))*

What to check: Each alert goes to a named person or team who reads it the same working day, and knows when to open the incident response plan.

Why: Detection is useful only if someone acts. 33 CFR 101.650(g)(2) asks for a cyber incident response plan that is developed, maintained and exercised.

Evidence to hold: [ ] Who receives the alerts, and their backup · [ ] The link between the alert and the incident response plan

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

eCFR, 33 CFR 101.650, Cybersecurity measures (US Coast Guard rule), in force since 16 July 2025, read on 11 November 2026. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.650

IMO, MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 28 May 2026. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

CISA, NSA, FBI, MS-ISAC and INCD, Guide to Securing Remote Access Software, 6 June 2023. https://www.cisa.gov/resources-tools/resources/guide-securing-remote-access-software

NSA and CISA, advisory AA23-278A, Top Ten Cybersecurity Misconfigurations, 5 October 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

OWASP API Security Top 10, 2023 edition. https://api-security.owasp.org/editions/2023/en/0x11-t10/

NIST SP 800-92, Guide to Computer Security Log Management, September 2006. https://csrc.nist.gov/pubs/sp/800/92/final

Microsoft, Event 4624: An account was successfully logged on, documentation read on 11 November 2026. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

Microsoft, Event 4732: A member was added to a security-enabled local group, documentation read on 11 November 2026. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4732

MITRE ATT&CK, T1021.001 Remote Services: Remote Desktop Protocol, read on 11 November 2026. https://attack.mitre.org/techniques/T1021/001/

MITRE ATT&CK, T1098 Account Manipulation, read on 11 November 2026. https://attack.mitre.org/techniques/T1098/

Port Cyber Alliance, Sigma rule pca_tos_rdp_logon_outside_admin_network.yml (DRL 1.1), 10 November 2026. https://portcyberalliance.org/detection-rules/sigma/windows/pca_tos_rdp_logon_outside_admin_network.yml

Port Cyber Alliance, Sigma rule pca_tos_member_added_to_local_administrators.yml (DRL 1.1), 10 November 2026. https://portcyberalliance.org/detection-rules/sigma/windows/pca_tos_member_added_to_local_administrators.yml

Port Cyber Alliance, open detection rules package (rules, sample events, tests, README, DRL 1.1), 10 November 2026. https://portcyberalliance.org/detection-rules/pca-detection-rules.zip

Detection rules

Lines D1 and D2 use the two open Sigma rules of Port Cyber Alliance: https://portcyberalliance.org/detection-rules/sigma/windows/pca_tos_rdp_logon_outside_admin_network.yml and https://portcyberalliance.org/detection-rules/sigma/windows/pca_tos_member_added_to_local_administrators.yml , with sample events and tests in https://portcyberalliance.org/detection-rules/pca-detection-rules.zip . The rules are licensed under their own licence, the Detection Rule License (DRL) 1.1, not under CC BY 4.0. Server names and address ranges in them are examples: replace them with your own.

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/best-practices/tos-access-hardening/ . Generic: no terminal, port, client or TOS vendor is named and no figure is invented. This checklist is not legal advice and does not replace your vendor's documentation. Port Cyber Alliance does not certify or audit terminals.