Detection of Impair Defenses through Disabled or Modified Tools across OS Platforms., Detection Strategy DET0497

Archived: 2026-04-05 14:19:48 UTC

AN1369

Detection of adversary behavior that disables or modifies security tools, including killing AV/EDR processes, stopping services, altering Sysmon registry keys, or tampering with exclusion lists. Defenders observe process/service termination, registry modification, and abnormal absence of expected telemetry.

Log Sources

Mutable Elements

Field	Description
ProcessNameExclusions	List of expected administrative tools/processes to prevent false positives.
TimeWindow	Defines correlation window linking process termination, registry edits, and service stoppage.
ServiceNames	Customizable list of security service names per enterprise deployment.

AN1370

Detection of adversaries attempting to stop or disable host-based security agents by killing daemons, unloading kernel modules, or modifying init/systemd service configurations.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: systemctl stop, service stop, or kill -9 on security daemons (e.g., falcon-sensor, auditd)
Service Metadata (DC0041)	auditd:CONFIG_CHANGE	delete: Modification of systemd unit files or config for security agents

Mutable Elements

Field	Description
AgentServiceNames	List of endpoint protection service names (varies across deployments).
AllowedAdminAccounts	Accounts permitted to legitimately stop or reconfigure services.

AN1371

Detection of adversary disabling endpoint security tools by unloading launch agents/daemons, modifying configuration profiles, or using security/uninstall commands to remove agents.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of launchctl unload, kill, or removal of security agent daemons
Service Metadata (DC0041)	macos:unifiedlog	Modification of system configuration profiles affecting security tools

Mutable Elements

Field	Description
DaemonNames	Expected security agent daemons (e.g., com.crowdstrike.falcon.Agent).
TimeWindow	Detection correlation period for multiple security tool disable actions.

AN1372

Detection of adversaries disabling cloud monitoring and logging agents such as CloudWatch, Google Cloud Monitoring, or Azure Monitor by API calls or agent process termination.

Log Sources

Mutable Elements

Field	Description
APIActions	Customizable list of cloud provider API calls related to monitoring/alerting disablement.
UserContext	Distinguishes adversary actions from authorized DevOps/CloudOps activities.

AN1373

Detection of adversaries tampering with container runtime security plugins, disabling admission controllers, or stopping monitoring sidecars.

Log Sources

Data Component	Name	Channel
Service Metadata (DC0041)	kubernetes:audit	kubectl delete or patch of security pods/admission controllers

Mutable Elements

Field	Description
NamespaceExclusions	Exclusion of namespaces where temporary deletion of monitoring tools is legitimate (e.g., staging).

AN1374

Detection of adversaries modifying startup configuration files to disable signature verification, logging, or monitoring features.

Log Sources

Data Component	Name	Channel
Service Metadata (DC0041)	networkdevice:config	write: Startup configuration changes disabling security checks

Mutable Elements

Field	Description
ConfigBaseline	Reference configuration state for detecting unauthorized modifications.
