

# Detection Strategy for Impair Defenses Across Platforms, Detection Strategy DET0317

Archived: 2026-04-05 17:48:39 UTC

## AN0886

Unusual service stop events, termination of AV/EDR processes, registry modifications disabling security tools, and firewall/defender configuration changes. Correlate process creation with service stop requests and registry edits.

### Log Sources

### Mutable Elements

Field	Description
ProcessWhitelist	Exclude authorized administrative tools that stop services during maintenance.
ServiceNamePatterns	Refine which services are considered security-critical (e.g., AV, EDR, firewall).

## AN0887

Execution of commands that stop or kill processes associated with logging or security daemons (auditd, syslog, falco). Detect modifications to iptables or disabling SELinux/AppArmor enforcement. Correlate sudo/root context with abrupt service halts.

### Log Sources

### Mutable Elements

Field	Description
ServiceList	Adjust monitored security service names depending on host configuration.
TimeWindow	Correlate multiple kill/stop events in short succession.

## AN0888

Execution of commands or APIs that disable Gatekeeper, XProtect, or system integrity protections. Detect configuration changes through unified logs. Monitor termination of system security daemons (e.g., sypolicyd).

### Log Sources

**Mutable Elements**

Field	Description
AdminToolWhitelist	Developers may legitimately disable Gatekeeper; whitelist approved contexts.

**AN0889**

Modification of container runtime security profiles (AppArmor, seccomp) or removal of monitoring agents within containers. Detect unauthorized mounting/unmounting of host /proc or /sys to disable logging or auditing.

**Log Sources**

**Mutable Elements**

Field	Description
RuntimeProfiles	Specify which security profiles should be monitored for modification.

**AN0890**

Unusual ESXi shell commands disabling syslog forwarding or stopping hostd/vpxa daemons. Detect modifications to firewall rules on ESXi host or disabling of lockdown mode.

**Log Sources**

**Mutable Elements**

Field	Description
LogDestination	Tune for environment-specific log forwarding hosts.

**AN0891**

Cloud control plane actions disabling security services (CloudTrail logging, GuardDuty, Security Hub). Detect IAM role abuse correlating with service disable events.

**Log Sources**

**Mutable Elements**

Field	Description
ServiceScope	Specify which cloud services (logging, monitoring, threat detection) must never be disabled.

**AN0892**

Changes to security configurations such as disabling MFA requirements, reducing session token lifetimes, or turning off risk-based policies. Correlate admin logins with sudden policy downgrades.

**Log Sources****Mutable Elements**

Field	Description
PolicyList	Adjust for the critical identity provider security policies to monitor.

**AN0893**

Execution of commands disabling AAA, logging, or security features on routers/switches. Detect privilege escalation followed by config changes that disable defense mechanisms.

**Log Sources**

Data Component	Name	Channel
<a href="#">Command Execution (DC0064)</a>	networkdevice:syslog	no logging buffered, no aaa new-model, disable firewall

**Mutable Elements**

Field	Description
CommandPatterns	Customize destructive command list per vendor platform.

**AN0894**

Disabling of security macros or safe mode settings within Word/Excel/Outlook. Detect registry edits or configuration file changes that weaken macro enforcement.

**Log Sources****Mutable Elements**

Field	Description
ApplicationScope	Specify which Office applications are monitored for macro security configuration changes.

Source: <https://attack.mitre.org/detectionstrategies/DET0317#AN0893>