Detection Strategy for Exploitation for Defense Evasion, Detection Strategy DET0595

Archived: 2026-04-05 17:35:31 UTC

AN1633

Detects exploitation attempts targeting defensive security software or OS services. Defender observation includes abnormal process behavior (e.g., AV or EDR crashing unexpectedly), unsigned/untrusted modules loaded into defensive processes, or privilege escalation from security agent services. Multi-event correlation ties exploitation attempts to subsequent evasive behavior like service termination or missing logs.

Log Sources

Mutable Elements

Field	Description
DefensiveProcessList	List of defensive services/processes (e.g., AV, EDR) monitored in the environment.
AllowedModulePaths	Whitelisted DLL/module paths normally loaded by defensive tools.
CrashThreshold	Number of abnormal terminations of defensive processes tolerated before triggering an alert.

AN1634

Detects kernel- or user-space exploitation attempts targeting auditd, AV daemons, or security monitoring agents. Defender observation includes unexpected segfaults, privilege escalation attempts from low-privileged processes, or modifications to security binaries. Correlates exploitation attempts with subsequent gaps in logging or terminated processes.

Log Sources

Mutable Elements

Field	Description
WatchedBinaries	List of critical security daemons (e.g., auditd, falco, AV agents) to monitor for exploitation.
CrashPatterns	Regex or patterns for kernel/syslog errors correlated with exploitation attempts.

AN1635

Detects exploitation of macOS security and integrity services, such as Gatekeeper, XProtect, or EDR agents. Defender observations include unsigned processes attempting privileged operations, abnormal termination of security daemons, or modification of system integrity logs.

Log Sources

Mutable Elements

Field	Description
SecurityDaemons	Monitored Apple and third-party EDR/AV daemon names.
UnsignedProcessThreshold	Number of unsigned high-privilege executions before alerting.

AN1636

Detects exploitation of IaaS cloud security boundaries to evade defense controls. Defender perspective includes anomalous API calls that bypass audit logging, disable monitoring, or manipulate guardrails (e.g., CloudTrail tampering). Correlation highlights when exploitation attempts precede sudden absence of expected telemetry.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	AWS:CloudTrail	StopLogging, DeleteTrail, UpdateTrail: API calls that disable or modify logging services

Mutable Elements

Field	Description
CriticalAPIs	List of sensitive cloud API operations that should be rare and tightly monitored.
TimeWindow	Duration for correlation of API exploitation with sudden logging gaps.

AN1637

Detects adversary abuse of SaaS platform vulnerabilities to bypass logging, monitoring, or consent boundaries. Defender perspective focuses on abnormal application integration events, missing audit logs, or API calls from unauthorized service principals that align with exploitation attempts.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	m365:unified	ApplicationModified, ConsentGranted: Unexpected app consent or modification events linked to security evasion

Mutable Elements

Field	Description
MonitoredApps	Applications and integrations expected in the environment; deviations may be suspect.
ConsentAnomalyThreshold	Threshold for anomalous OAuth or app consent events before flagging exploitation.

Source: https://attack.mitre.org/detectionstrategies/DET0595#AN1635