Multi-Platform Execution Guardrails Environmental Validation Detection Strategy, Detection Strategy DET0562

Archived: 2026-04-05 17:37:53 UTC

AN1551

Windows environmental validation behavioral chain: (1) Rapid system discovery reconnaissance through WMI queries, registry enumeration, and network share discovery, (2) Environment-specific artifact collection (hostname, domain, IP addresses, installed software, hardware identifiers), (3) Cryptographic operations or conditional logic based on collected environmental values, (4) Selective payload execution contingent on environmental validation results, (5) Temporal correlation between discovery activities and subsequent execution or network communication

Log Sources

Mutable Elements

Field	Description
DiscoveryTimeWindow	Maximum time window for correlating multiple discovery activities indicating reconnaissance phase - adjust based on normal system behavior (default: 300 seconds)
DiscoveryActivityThreshold	Minimum number of different discovery techniques within time window to trigger detection - balance between false positives and coverage (default: 4 activities)
CryptographicLibraryWhitelist	Approved cryptographic libraries and modules for legitimate organizational use - maintain based on approved software inventory
WMIQueryComplexityThreshold	Complexity score for WMI queries indicating reconnaissance vs. legitimate administration - tune based on administrative patterns
EnvironmentalArtifactList	Environment-specific values commonly targeted by guardrails (hostnames, domains, network shares) - customize for organizational environment
ExecutionDelayBaseline	Statistical baseline for normal delay between discovery and execution activities - establish through historical analysis

AN1552

Linux environmental validation behavioral chain: (1) Intensive system enumeration through command execution (uname, hostname, ifconfig, lsblk, mount), (2) File system reconnaissance targeting specific paths, network configurations, and installed packages, (3) Process and user enumeration to validate target environment characteristics, (4) Conditional script execution or binary activation based on environmental criteria, (5) Network connectivity validation and external IP address resolution for geolocation verification

Log Sources

Mutable Elements

Field	Description
SystemDiscoveryCommandList	Linux commands commonly used for system reconnaissance - customize based on environment-specific discovery patterns
ReconnaissanceBurstThreshold	Number of discovery commands within time window indicating reconnaissance burst - tune based on legitimate administrative activity
EnvironmentalCheckPatterns	File paths and system properties commonly validated by environmental keying - adapt to organizational infrastructure
NetworkDiscoveryBaseline	Normal network discovery activity patterns to distinguish from malicious reconnaissance
ConditionalExecutionIndicators	Script patterns and conditional logic indicating environment-based execution decisions

AN1553

macOS environmental validation behavioral chain: (1) System profiling through system_profiler, sysctl, and hardware discovery commands, (2) Network interface and configuration enumeration for geolocation and network environment validation, (3) Application installation and version discovery for software environment fingerprinting, (4) Security feature detection (SIP, Gatekeeper, XProtect status), (5) Conditional payload execution based on macOS-specific environmental criteria and System Integrity Protection bypass validation

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	process execution events for system discovery utilities (system_profiler, sysctl, networksetup, ioreg) with parameter analysis

Data Component	Name	Channel
File Access (DC0055)	fs:fileevents	File system access events with kFSEventStreamEventFlagItemRemoved, kFSEventStreamEventFlagItemRenamed flags for environmental artifact collection (/System/Library, /usr/sbin, plist files)

Mutable Elements

Field	Description
MacOSDiscoveryTools	macOS-specific system discovery utilities commonly used for environmental validation
SecurityFeatureEnumeration	Security features and configurations typically validated by macOS execution guardrails
HardwareFingerprintBaseline	Normal hardware discovery patterns to distinguish from environmental validation attempts
SIPBypassIndicators	Patterns indicating attempts to validate or bypass System Integrity Protection

AN1554

ESXi hypervisor environmental validation behavioral chain: (1) Virtual machine inventory and configuration enumeration through vim-cmd and esxcli commands, (2) Host hardware and network configuration discovery for hypervisor environment validation, (3) Datastore and storage configuration reconnaissance, (4) vCenter connectivity and cluster membership validation, (5) Selective malware deployment based on virtualization infrastructure characteristics and target VM validation

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	esxi:shell	shell command execution for system discovery (vim-cmd, esxcli, vmware-cmd) targeting VM inventory and host configuration
Process Creation (DC0032)	esxi:hostd	host daemon events related to VM operations and configuration queries during reconnaissance

Mutable Elements

Field	Description
ESXiDiscoveryCommands	ESXi commands commonly used for hypervisor and VM reconnaissance
VMInventoryEnumerationThreshold	Number of VM inventory queries within time window indicating reconnaissance activity
HypervisorEnvironmentBaseline	Normal hypervisor management activity patterns for distinguishing malicious reconnaissance
DatastoreAccessPatterns	Unusual datastore access patterns indicating environmental validation or target selection

---