Detection Strategy for Exfiltration Over Webhook, Detection Strategy DET0153

Archived: 2026-04-05 15:32:52 UTC

AN0436

Unusual processes (e.g., powershell.exe, wscript.exe, mshta.exe) posting data to webhook endpoints (Discord, Slack, webhook.site) using HTTP POST/PUT requests. Defender perspective: suspicious process lineage followed by outbound HTTPS traffic to webhook domains.

Log Sources

Mutable Elements

Field	Description
WebhookDomains	Domains to monitor such as discord.com/api/webhooks, slack.com/api, webhook.site.
UploadSizeThreshold	Threshold for abnormal data sent via webhook requests.
ApprovedApps	List of approved business apps using webhooks to reduce noise.

AN0437

Processes such as curl, wget, or custom scripts initiating POST requests to webhook endpoints with encoded or bulk data. Defender perspective: abnormal chaining of file compression or access followed by outbound data to webhook URLs.

Log Sources

Mutable Elements

Field	Description
AllowedTools	Expected command-line utilities allowed to interact with webhooks in enterprise environments.
TimeWindow	Expected timeframe for legitimate webhook traffic (e.g., CI/CD deployments).

AN0438

Unexpected apps or scripts (osascript, curl, Automator workflows) exfiltrating data via webhooks. Defender perspective: correlation of clipboard/file read operations followed by HTTPS POST traffic to webhook services.

Log Sources

Mutable Elements

Field	Description
WebhookEndpoints	Webhook URLs monitored for exfiltration.
EntropyThreshold	High entropy payloads may indicate encoded/encrypted exfiltration.

AN0439

VMware services or management daemons generating HTTP POST requests to webhook endpoints, chained with unusual datastore or log access. Defender perspective: exfiltration from VM logs or disk images over webhook URLs.

Log Sources

Mutable Elements

Field	Description
DatastoreExfilThreshold	Minimum data volume to flag exfiltration attempts from VM files.
ApprovedIntegrations	Whitelisted CI/CD or automation webhooks tied to vSphere/ESXi.

AN0440

Suspicious SaaS tenant activity involving webhook configurations pointing to external or untrusted domains. Defender perspective: repeated automated exports or suspicious webhook endpoint registrations.

Log Sources

Mutable Elements

Field	Description
WebhookRegistrations	Monitor new webhook creation events in SaaS environments.
ExternalDomains	Flag webhooks pointing to domains not owned by the enterprise.
