Network Logging

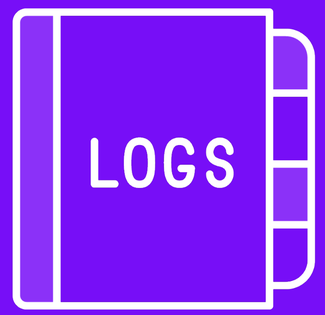


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

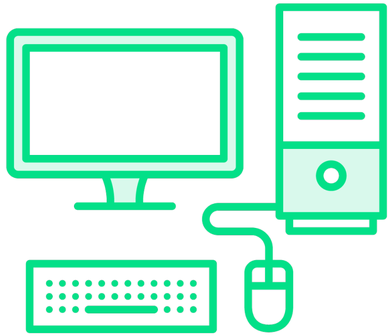
What's the Purpose of Logging?



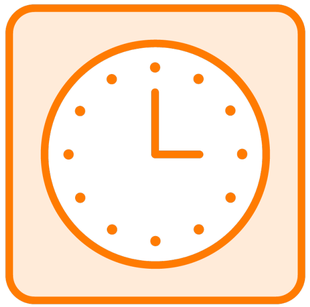
Logging involves recording events, actions, users, locations, and time to support the monitoring of malicious activity.



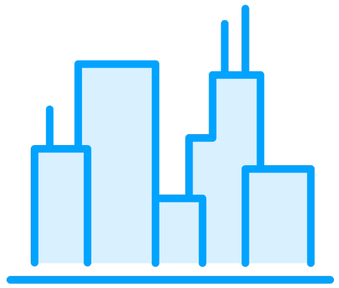
Who



What



When



Where

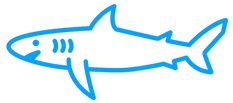


Why

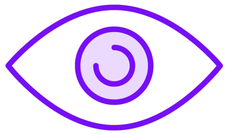
Packet Capture



Network interface logging



Network Device, WireShark, TCPdump, or NetMon

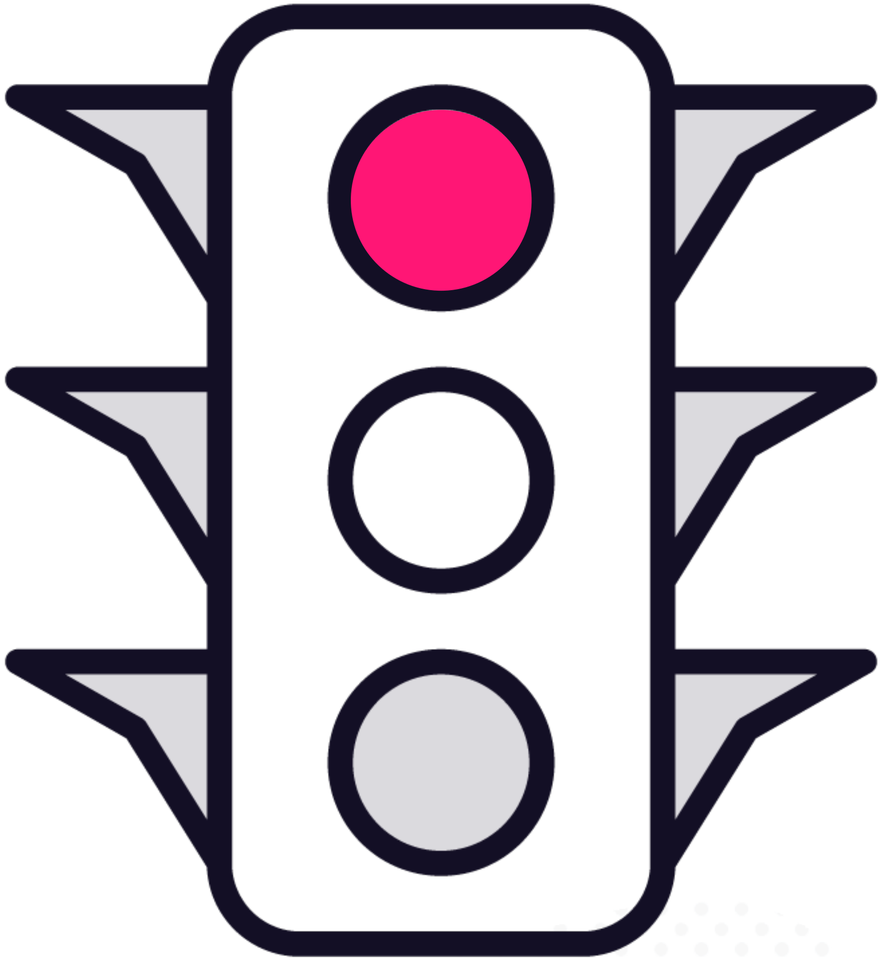


Detailed low-level logging



Security and performance investigations

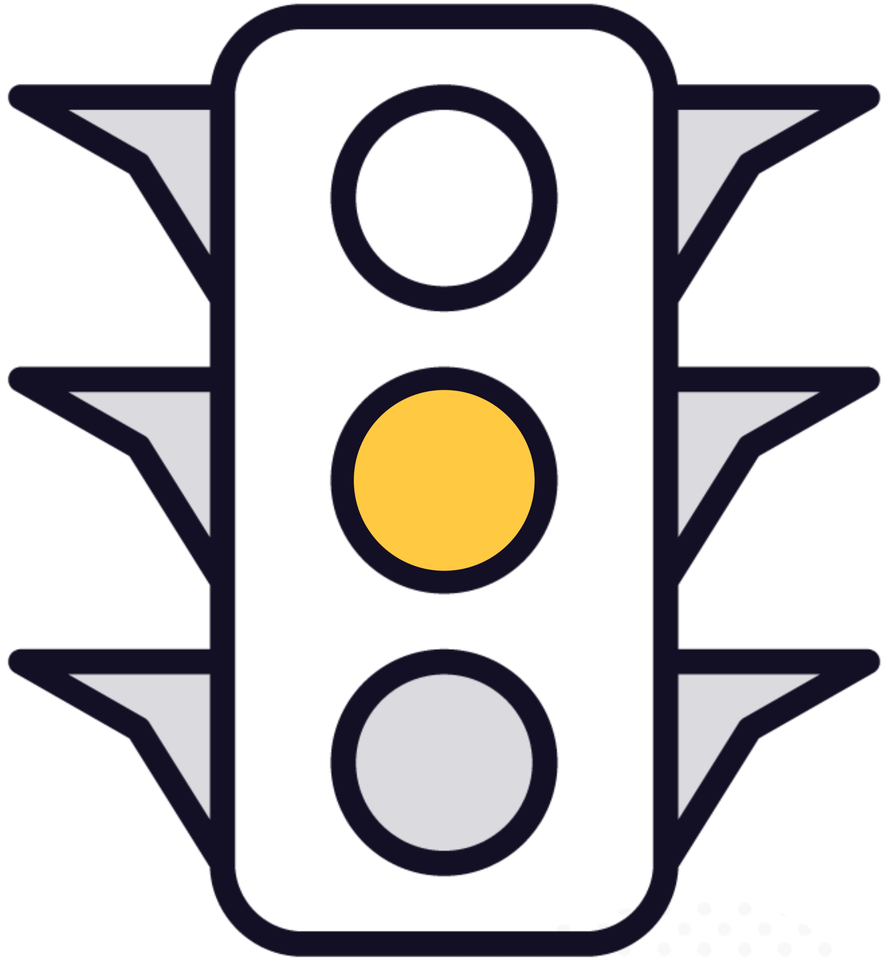
Network Traffic Logs



High-level network traffic logging



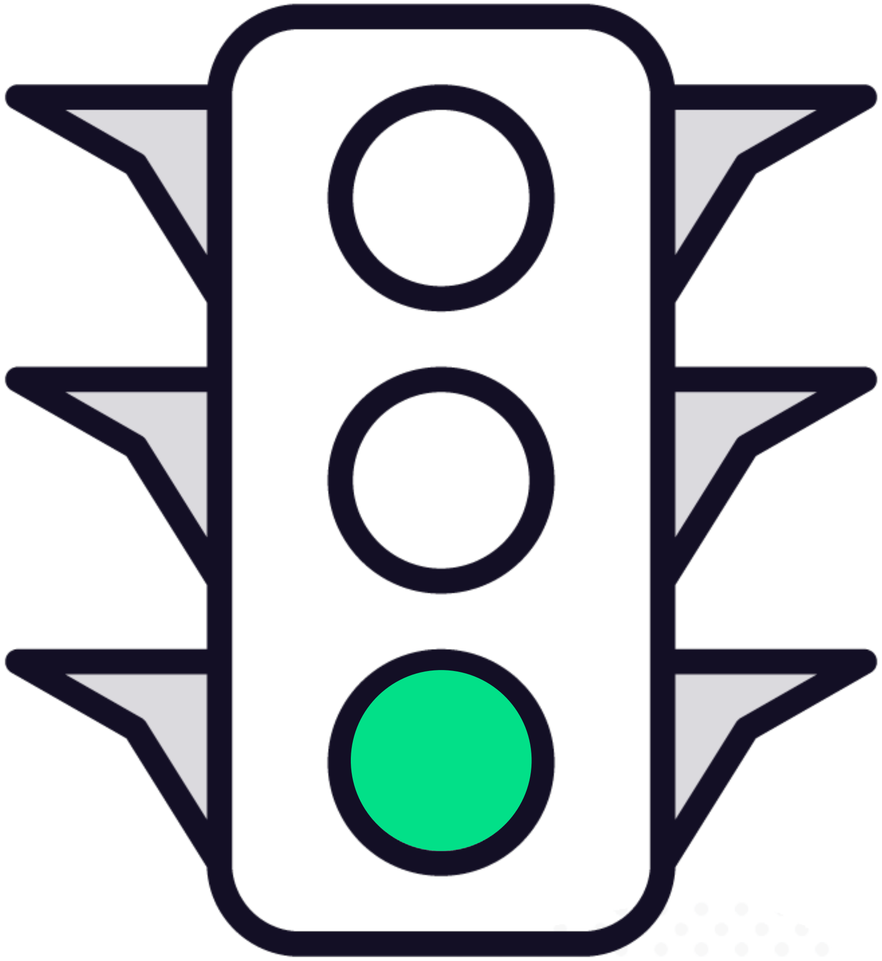
Network Traffic Logs



High-level network traffic logging

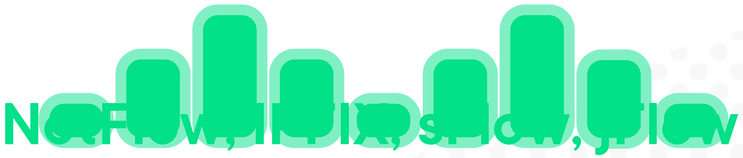
Source	Destination	Port	Protocol
10.0.5.50	54.71.221.199	TCP 443	HTTPS
192.168.1.36	192.168.1.6	TCP 22	SSH

Network Traffic Logs

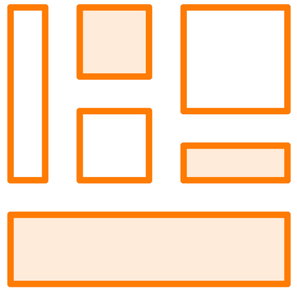


High-level network traffic logging

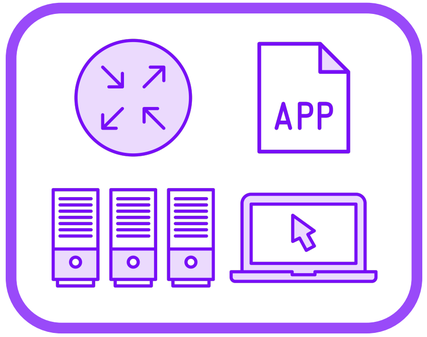
IP, port, protocol, and flow information



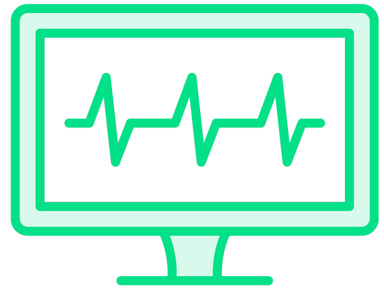
Network Traffic Logs



Cache, collector, and export location

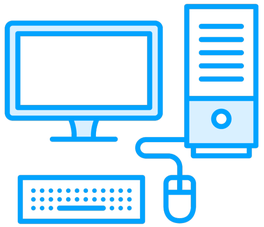


Devices, apps, and endpoints



Provides data for monitoring

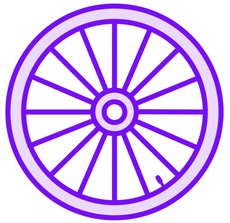
Logging Considerations



Classify Assets



Adjust Log Levels

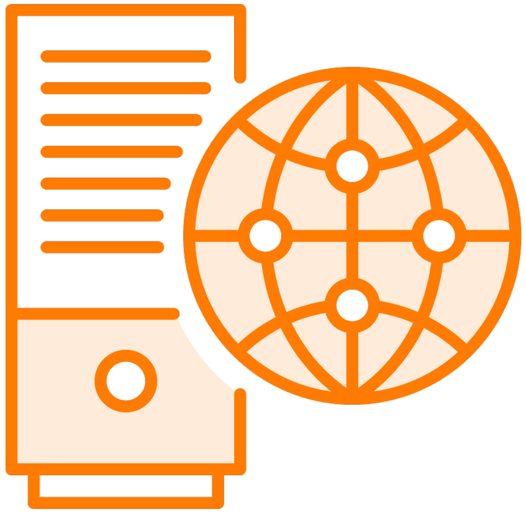


Compliance Requirements



Test Effectiveness

Centralized Network Logging



Simple Network Management Protocol



Security Information and Event Management

Security Information and Event Management (SIEM)



Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

SIEM



Sources



Query

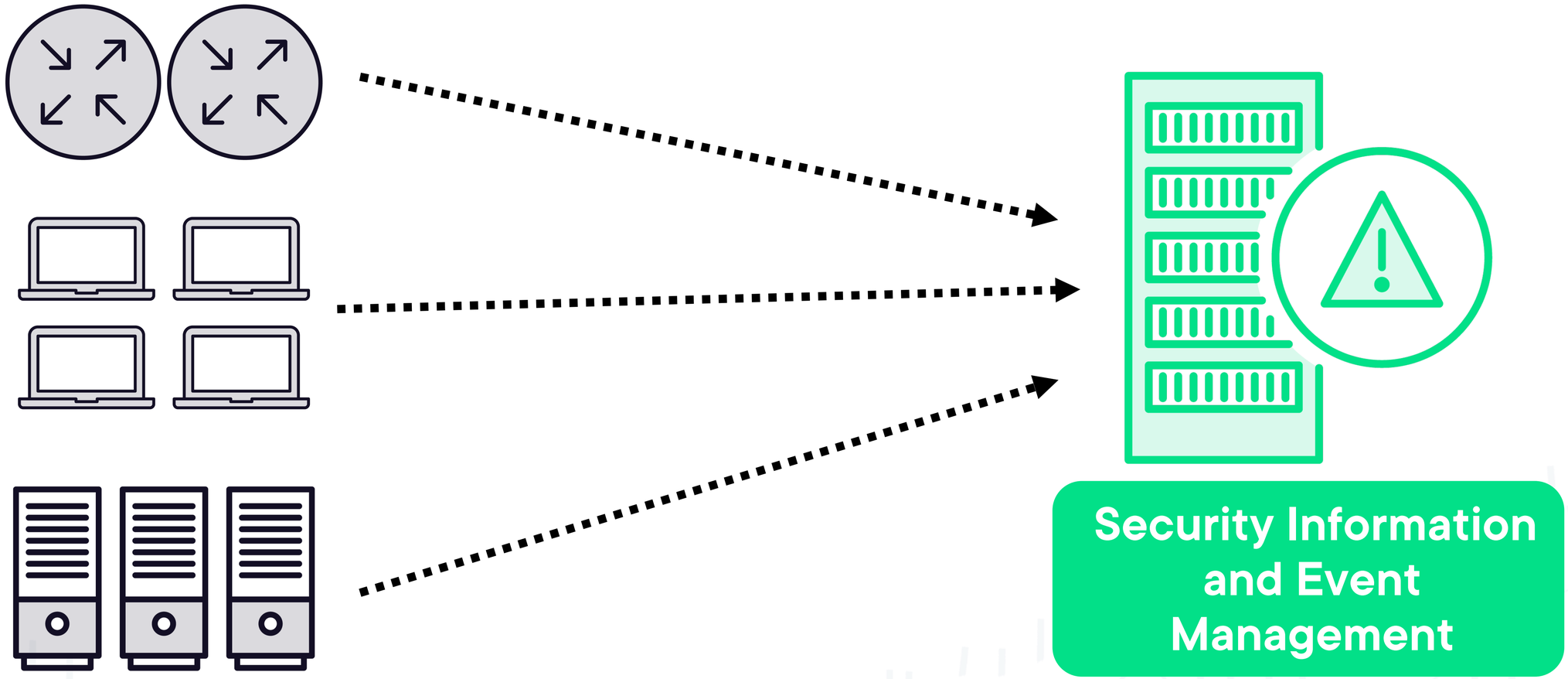


Alerts



Dashboards

Log Sources

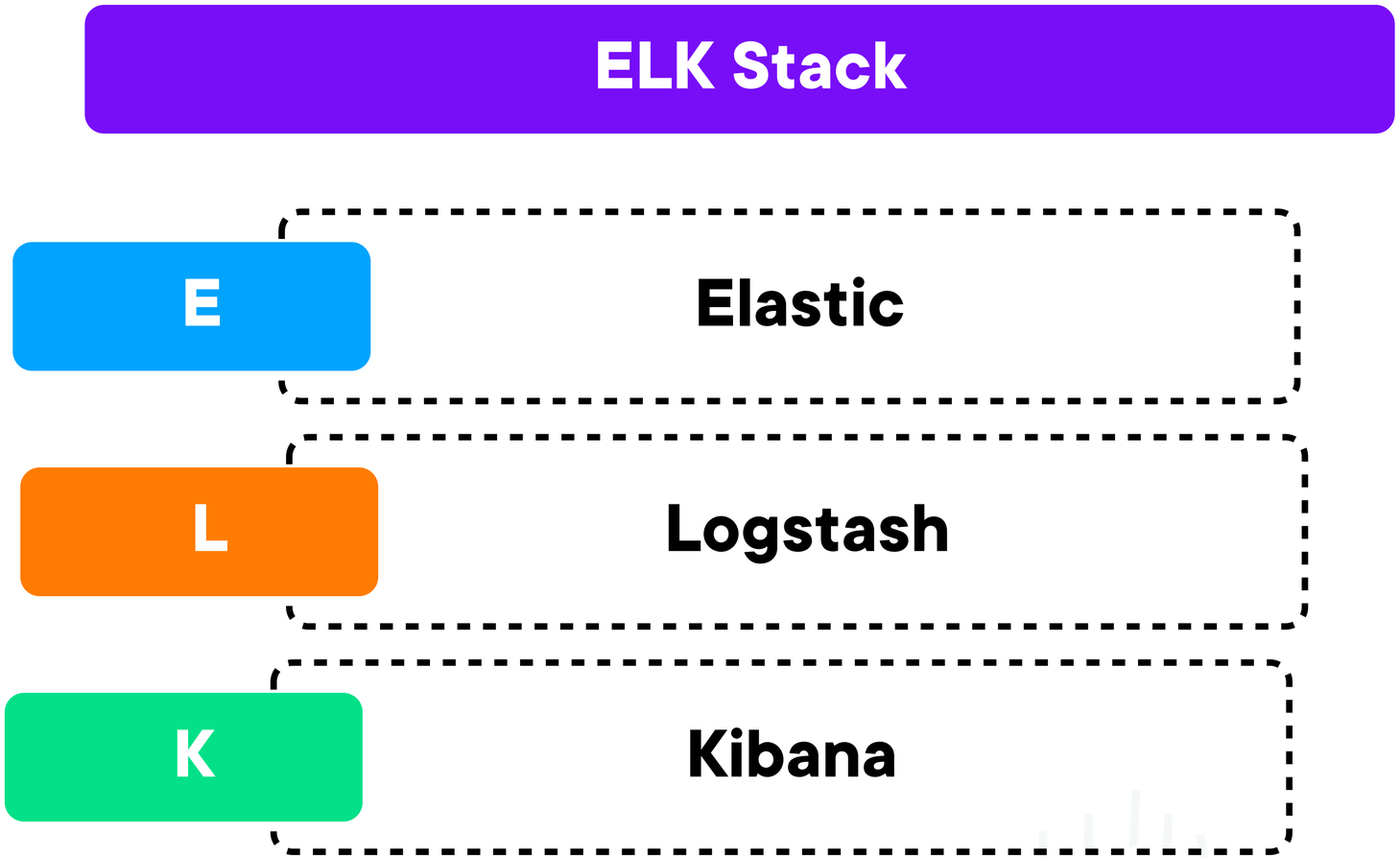


Queries

Splunk: Failed Authentication Attempts

```
index=wineventlog sourcetype="WinEventLog:Security"
EventCode=4625
| stats count by Account_Name, ComputerName, IpAddress, Message
| rename count as "Failed Authentication Attempts"
| sort - "Failed Authentication Attempts"
```

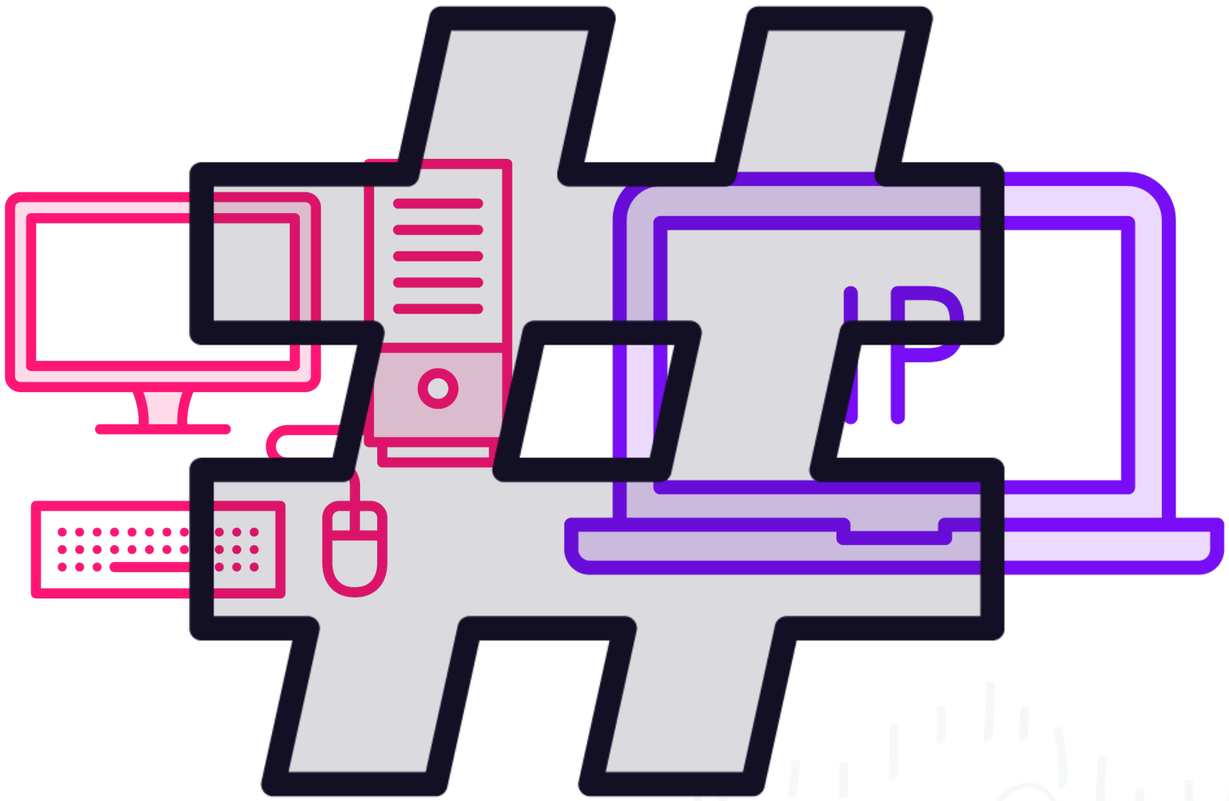
Queries



Queries



Failed Authentication Attempts



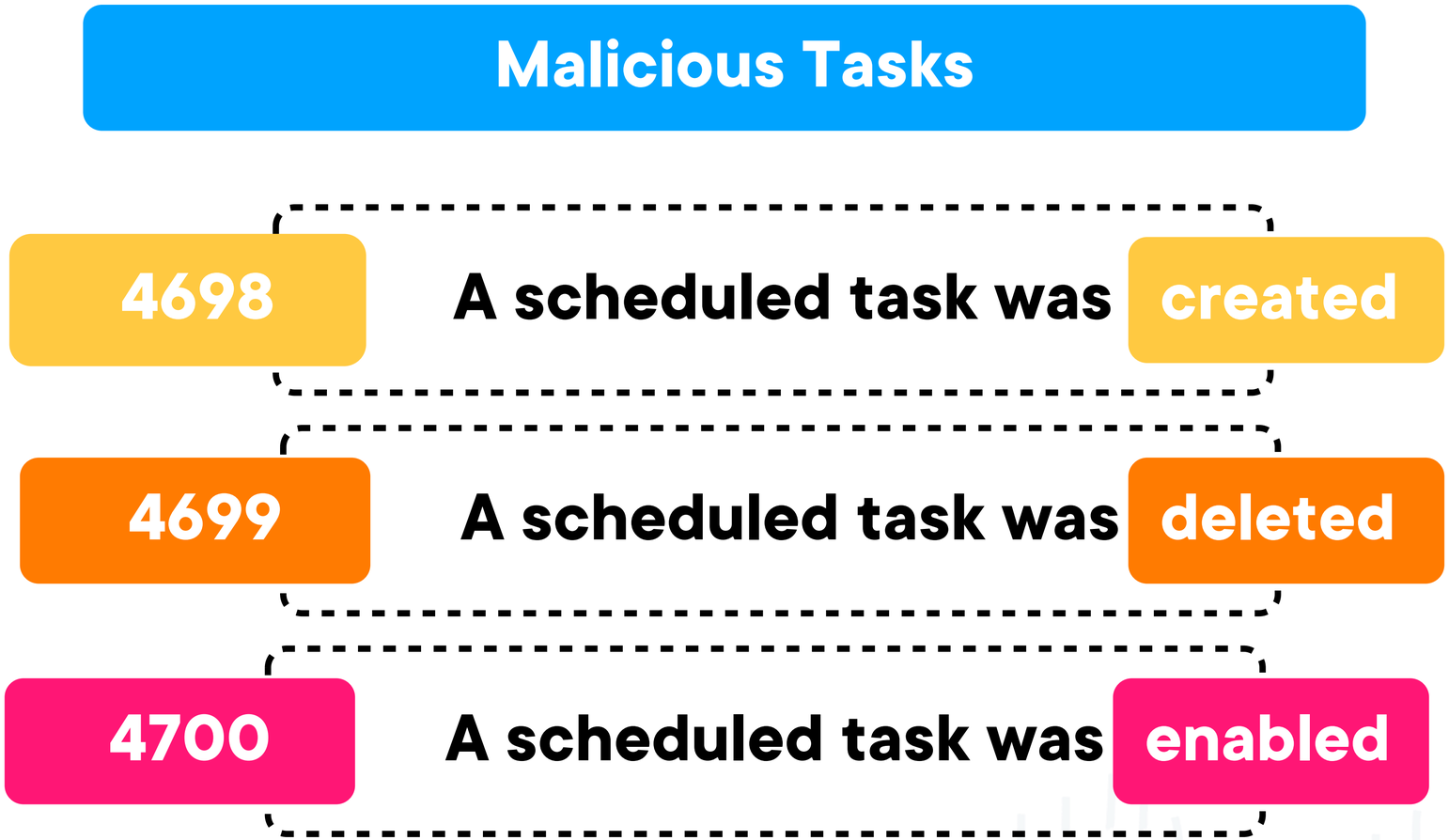


Queries

Splunk: Malicious Tasks

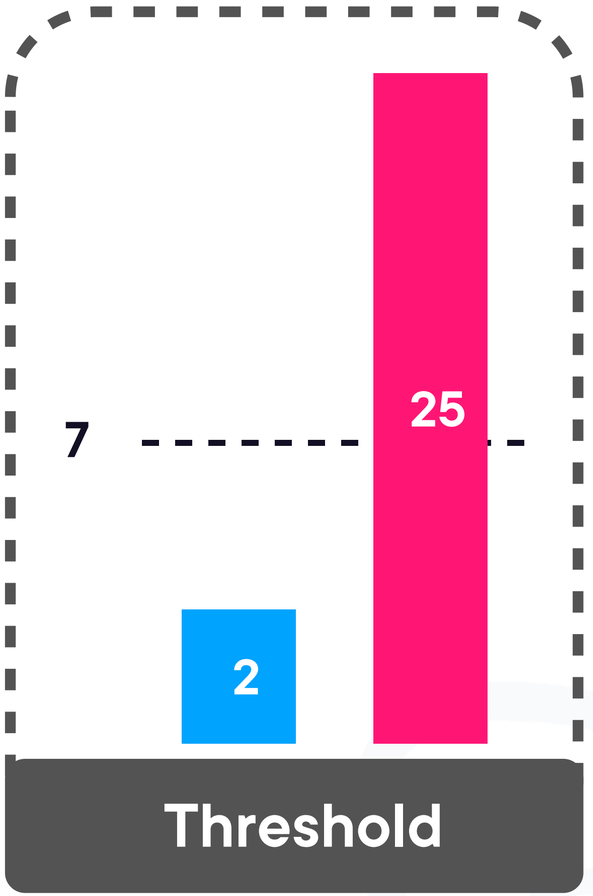
```
index=wineventlog sourcetype="WinEventLog:Security"
(EventCode=4698 OR EventCode=4699 OR EventCode=4700)
| stats count by EventCode, Account_Name, ComputerName, Message
| rename count as "Scheduled Task Events"
| sort - "Scheduled Task Events"
```

Queries


Malicious Tasks
4698
A scheduled task was
created
4699
A scheduled task was
deleted
4700
A scheduled task was
enabled

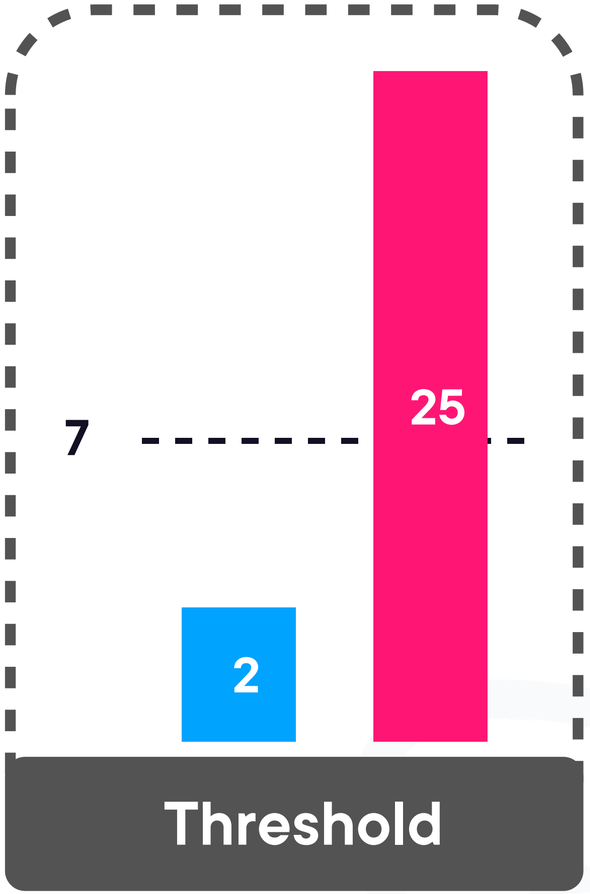
Alerts



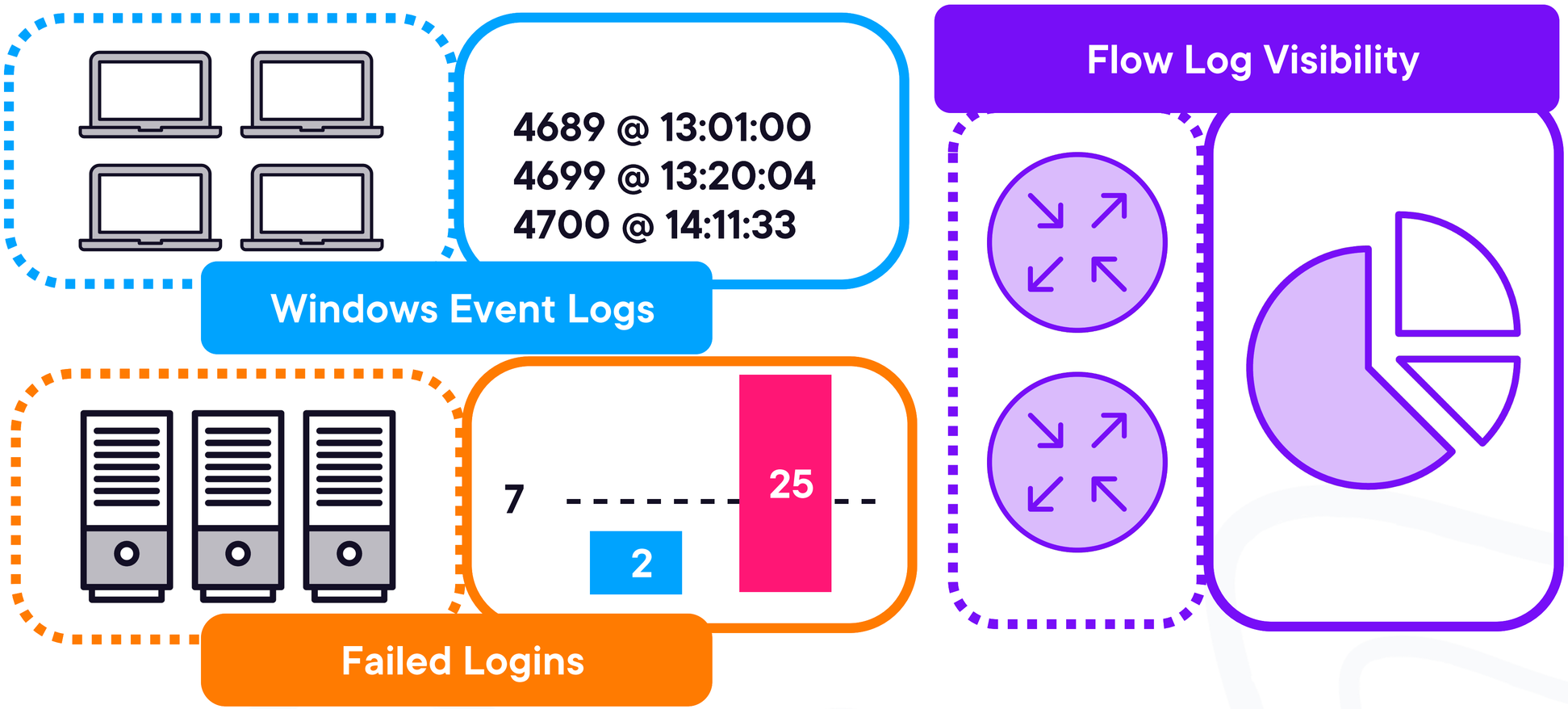


Alerts





Dashboards


4689 @ 13:01:00
4699 @ 13:20:04
4700 @ 14:11:33
Windows Event Logs
7
25
2
Failed Logins
Flow Log Visibility

Network Intrusion Detection and Prevention

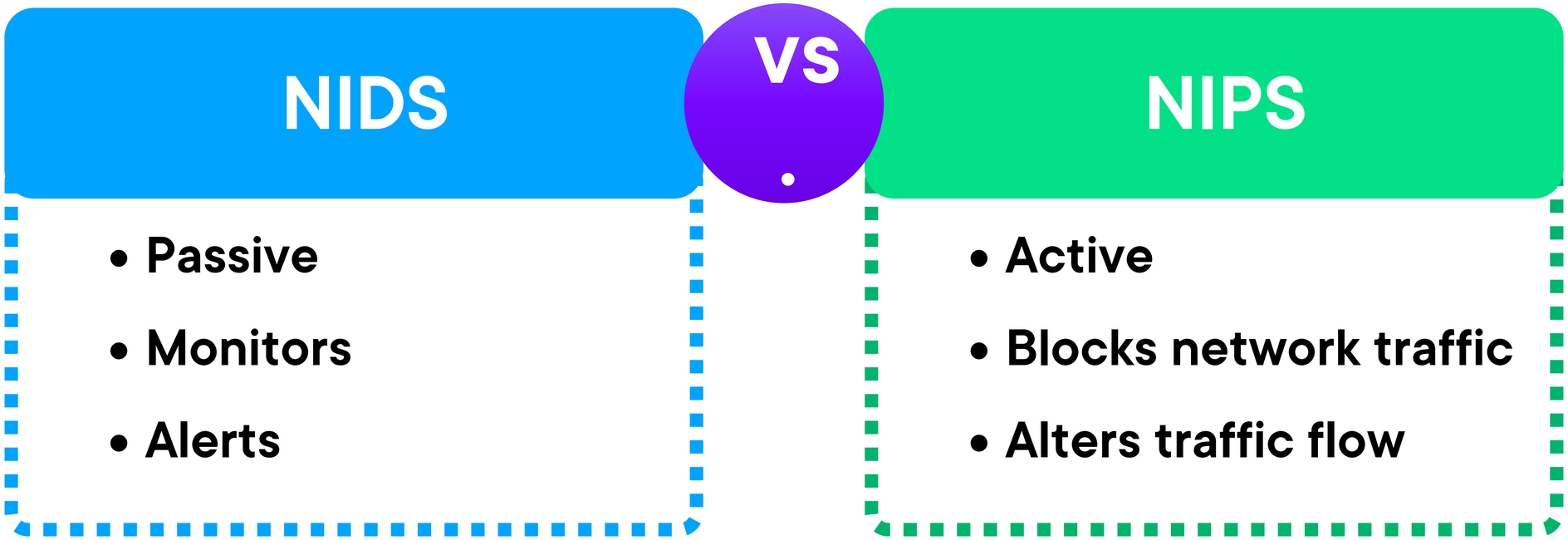


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

NIDS vs. NIPS


NIDS
VS
NIPS
• Passive
• Monitors
• Alerts
• Active
• Blocks network traffic
• Alters traffic flow

Snort



Real-time

Rules

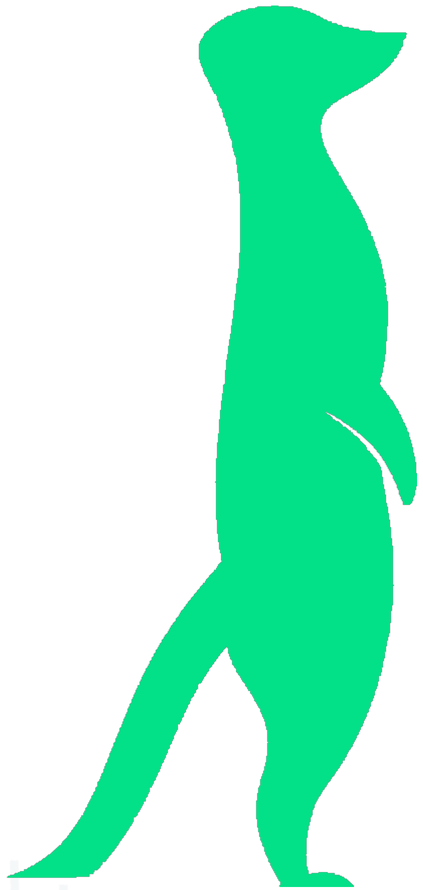
Detection

Snort

RDP Brute Force Attempt

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"RDP brute force
attempt"; flow:to_server,established; threshold: type threshold,
track by_src, count 5, seconds 60; sid:1000003; rev:1;)
```

Suricata



More than IDS/IPS

Rules and Detections

Rulesets

Suricata

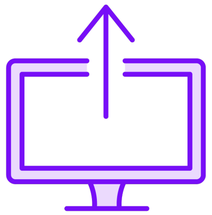
C2 Traffic Flow

```
alert http any any -> any any (msg:"Malware: Traffic flow to known
Ransomware C2 server"; flow:established;
content:"malicious_domain.com"; http_host; sid:200002;)
```

Suspicious Activity



Initial and Unusual Access



Data Exfiltration Activity



Credential Abuse



Indicators of Compromise (IoC)

Network Security Monitoring



Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Zeek



Network Security Monitoring

Signature and Behavior

Scripts

Zeek

```
@load base/protocols/conn
@load base/frameworks/files/hash
```

```
malicious_hashes: set[string] =
{
 “malicious_hash”
};
```

Load Base Scripts

List Malicious Hashes

```
event file_hash(f: fa_file, kind: string, hash: string)
{if (hash in malicious_hashes)
{local msg = fmt(“ALERT: malicious hash", f$source, hash); print msg;}
```

Zeek

```
event file_new(f: fa_file)
{
 Files::add_analyzer(f,Files::ANALYZER_SHA256);
}
```

Analyze File Hashes

Zeek



Network Security Monitoring

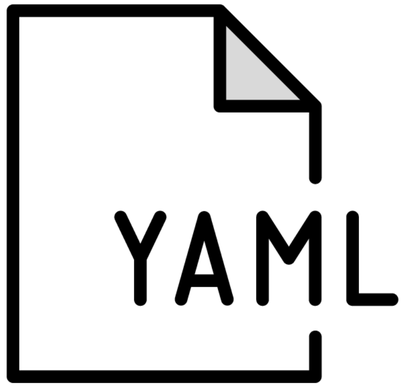
Signature and Behavior

Scripts

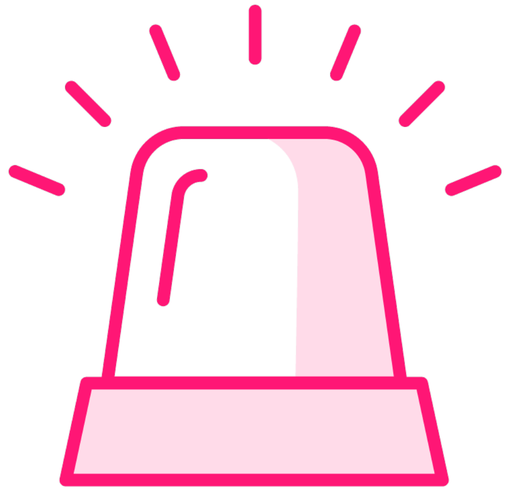
Sigma



Open Signature Format



YAML-based



Sharing Detections

Sigma (CVE-2024-37085)

```
title: Potential Exploitation of CVE-2024-37085 - Suspicious Creation Of ESX Admins Group
id: c408acfe-2870-41df-8d2f-9f4daa4555ed
status: experimental
description: Detects execution of the "net.exe" command in order to add a group named "ESX Admins".
This could indicates a potential exploitation attempt of CVE-2024-37085, which allows an attacker to
elevate their privileges to full administrative access on an domain-joined ESXi hypervisor.
VMware ESXi hypervisors joined to an Active Directory domain consider any member of a domain group
named "ESX Admins" to have full administrative access by default.
references:
    - https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-
hypervisor-vulnerability-for-mass-encryption/
author: frack113
date: 2024/07/29
tags:
    - attack.execution
    - cve.2024.37085
    - detection.emerging_threats
```

CVE-2024-37085

Sigma (CVE-2024-37085)

Log Source

```
logsource:
  category: process_creation
  product: windows
```

Sigma (CVE-2024-37085)

Detection and Selection

```
detection:
    selection_net_img:
        - Image|endswith:
            - '\net.exe'
            - '\net1.exe'
        - OriginalFileName:
            - 'net.exe'
            - 'net1.exe'
```

Selection

```
selection_net_cmd:
    CommandLine|contains|all:
        - '/add'
        - '/domain'
        - 'ESX Admins'
        - 'group'
```

Sigma (CVE-2024-37085)

Selection

```
selection_powershell_img:
  - Image|endswith:
    - '\PowerShell.exe'
    - '\pwsh.exe'
  - OriginalFileName:
    - 'PowerShell.exe'
    - 'pwsh.dll'
```

Selection

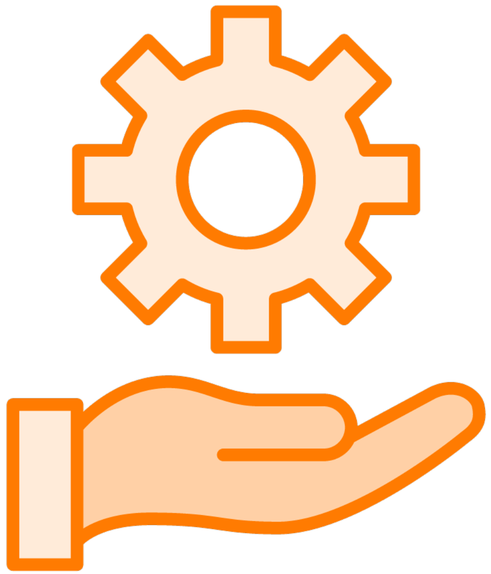
```
selection_powershell_cli:
  CommandLine|contains|all:
    - 'New-ADGroup'
    - 'ESX Admins'
```

Sigma (CVE-2024-37085)

Conditions

```
    condition: all of
selection_net_* or all of
selection_powershell_*
  falsepositives:
    - Unknown
  level: high
```

Detection-as-Code (DaC)



Automation

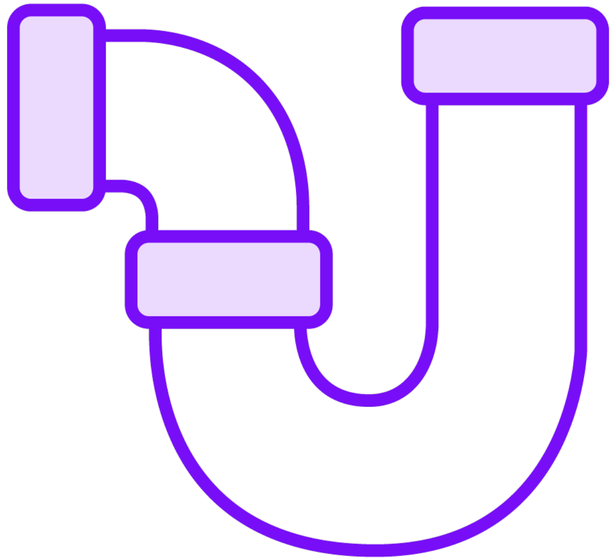


Up-to-date
Detection Rules



New Threats

Detection-as-Code (DaC)



CI/CD

Adversarial Tactics, Techniques, and Procedures (TTP)

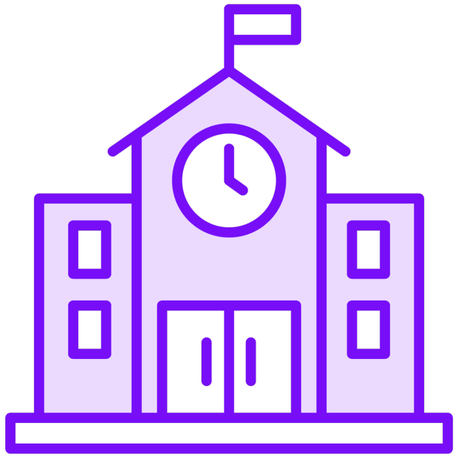


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Frameworks

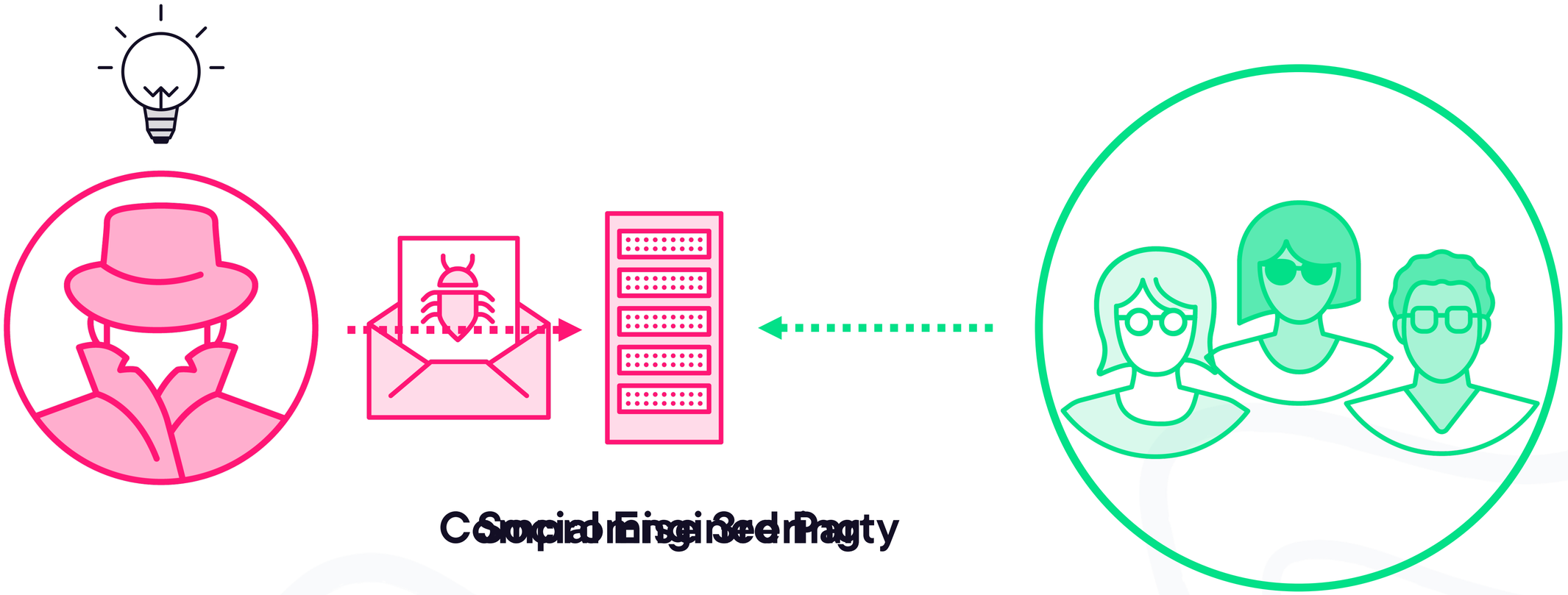


MITRE ATT&CK®



Lockheed Martin
Cyber Kill Chain

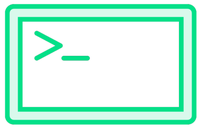
First Contact



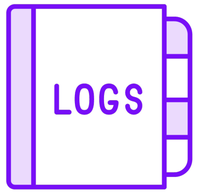
Under the Radar



Boot Scripts and Scheduled Tasks



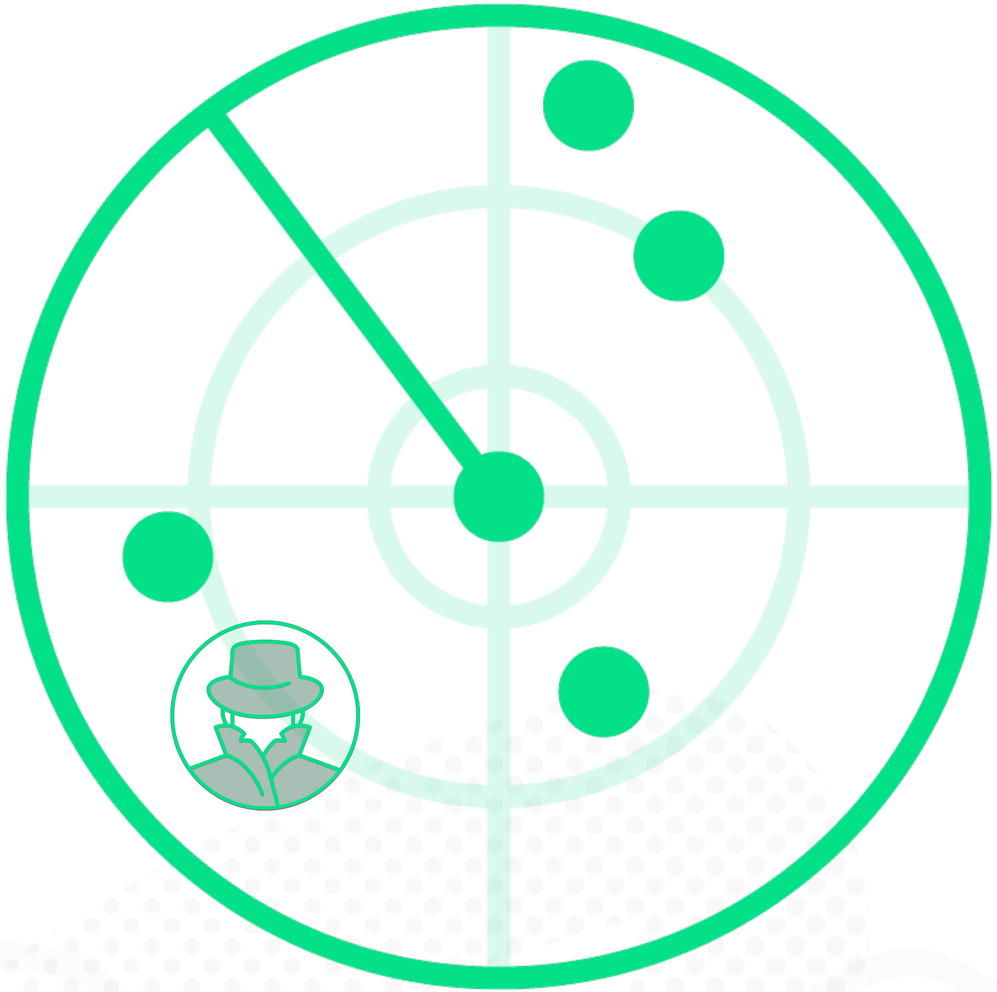
Utilize Environmental Tools



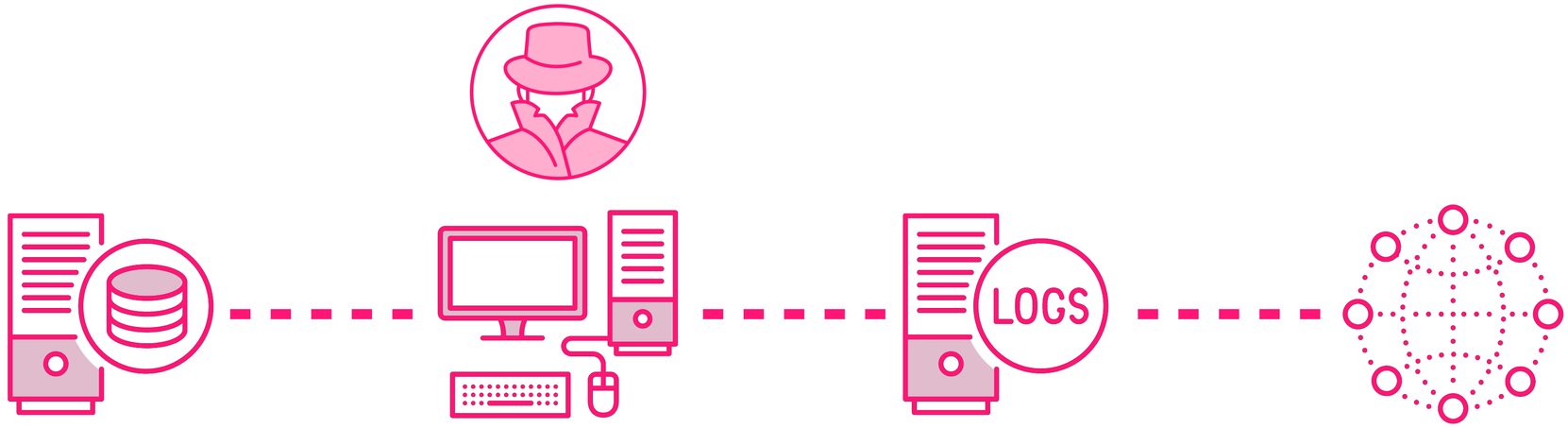
Disable Logging



Patch DC Authentication

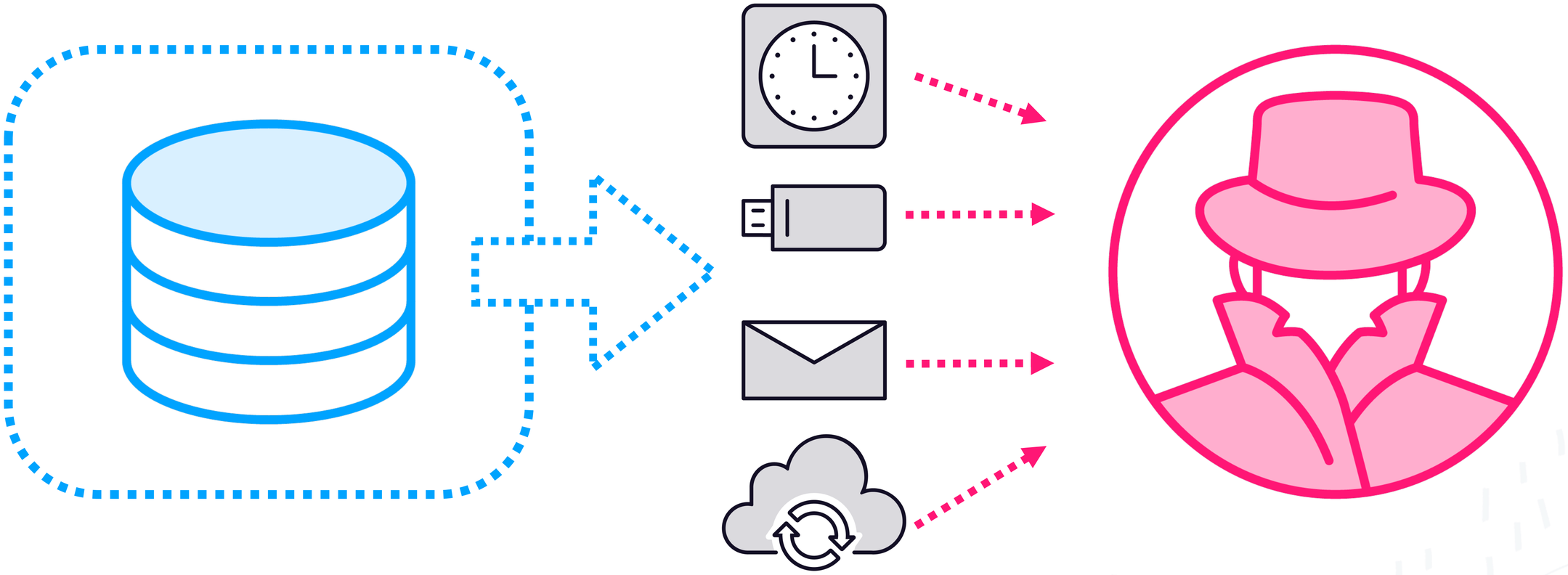


Movement Through Network

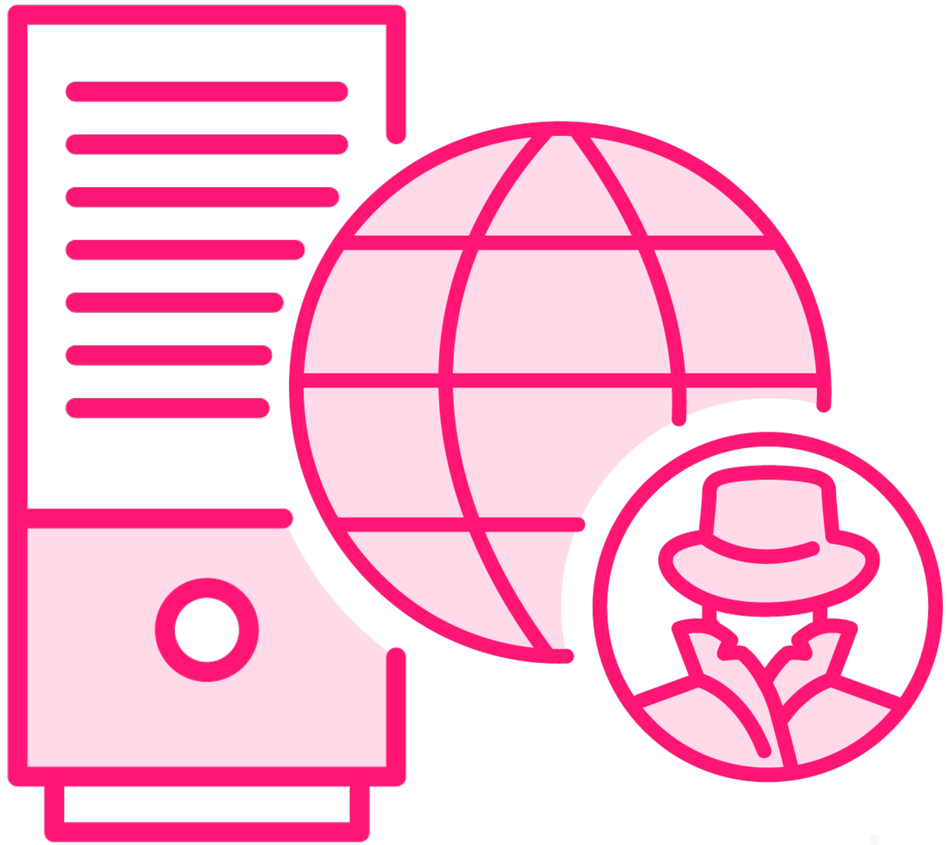


Credentials and Data Pivot Point Evasion Enumeration

End Game



End Game



Honeynets

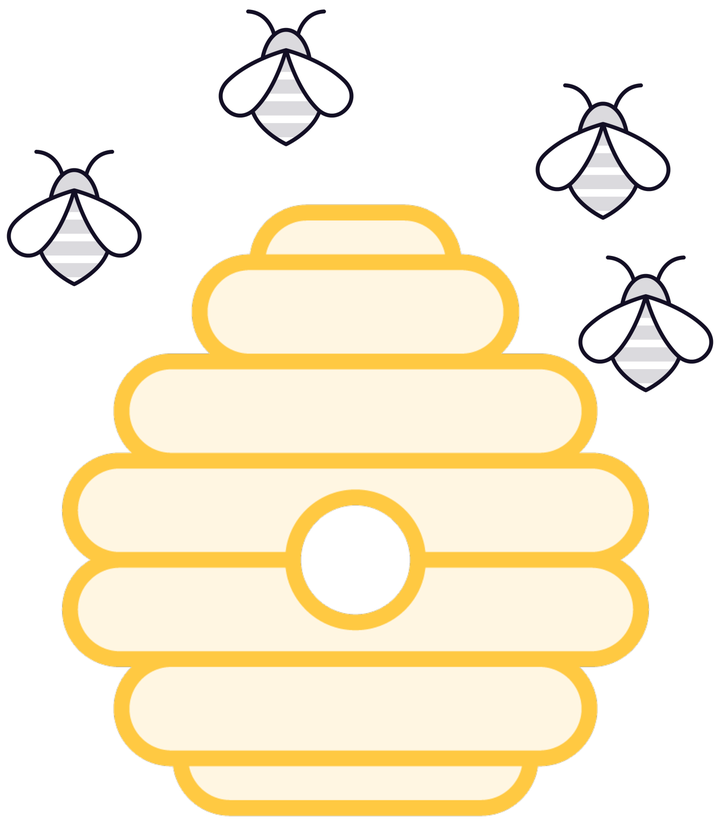


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Honeypot



Lure

Isolated

Interactivity

Track



Honeynet



Decoy



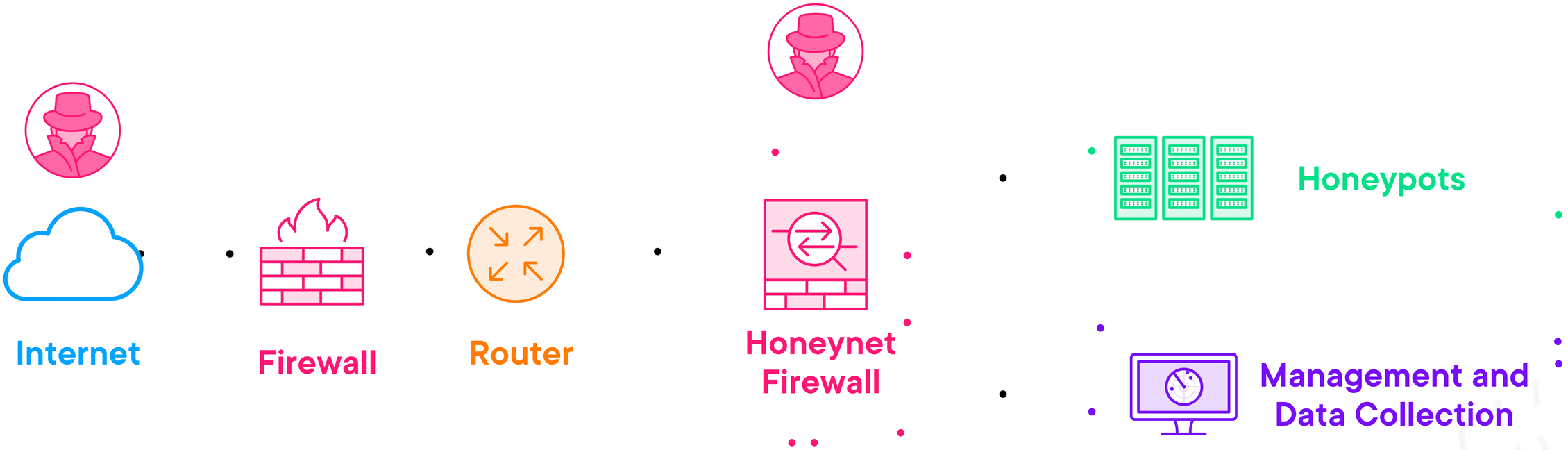
Track



TTP



Honeynet Architecture



Compliance Considerations



Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Governance, Risk and Compliance (GRC)



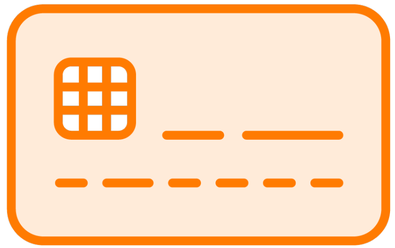
Security Frameworks



Healthcare



Global



Payment Card

PCI-DSS

