SANS

A Log Lifecycle

Security operations aren't suffering from a "big data" problem – but rather a "data analysis" problem. A SIEM can be an incredibly valuable tool for the SOC when implemented correctly. Leverage the Log Lifecycle Poster to add context and enrich data to achieve actionable intelligence – enabling detection techniques that do not exist in your environment today.

Log Information

Windows Log Channels

- Application
- Security
- System
- Powershell
- Sysmon
- AppLocker
- Firewall
- Driver Frameworks
- User Mode

Linux/Unix Logs

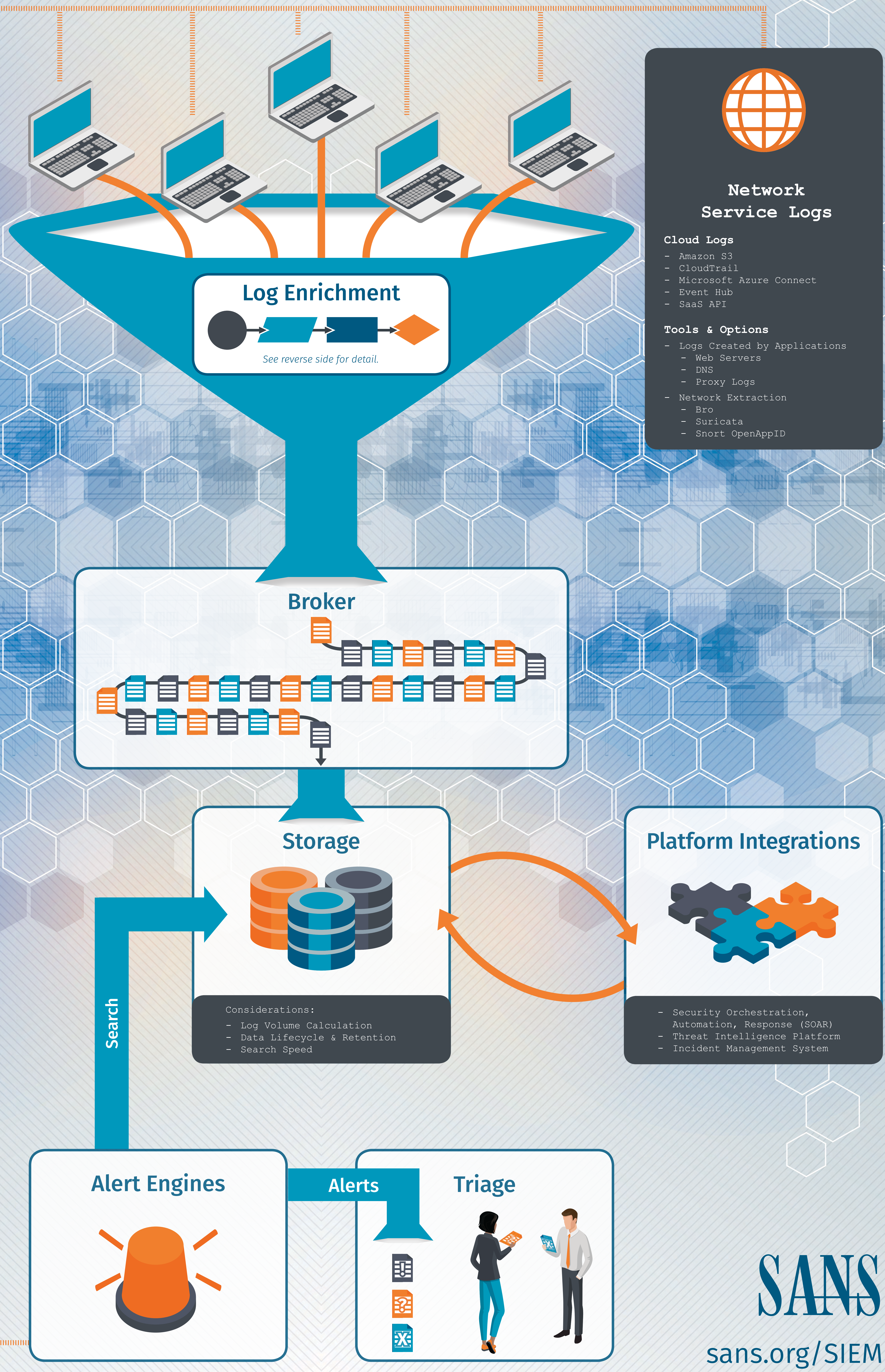
- auth.log
- firewall
- audit.log
- messages.log

Log Collection Types

- Agents
- 3rd Party
- OS Built In
- Agentless
- Scripting

Log Formats

- Unstructured Text
- CSV
- Key Value
- JSON
- CEF
- LEEF



Network Service Logs

Cloud Logs

- Amazon S3
- CloudTrail
- Microsoft Azure Connect
- Event Hub
- SaaS API

Tools & Options

- Logs Created by Applications
  - Web Servers
  - DNS
  - Proxy Logs
- Network Extraction
  - Bro
  - Suricata
  - Snort OpenAppID

Storage

Considerations:

- Log Volume Calculation
- Data Lifecycle & Retention
- Search Speed

Platform Integrations

- Security Orchestration, Automation, Response (SOAR)
- Threat Intelligence Platform
- Incident Management System

Rule Logic

Search Query

- Alert on anything that matches the search query parameters.

Blacklist

- Alert any time a field matches on any of the terms on the given list.

Whitelist

- Alert any time a field does not match an item on the given list.

First Sighting / New Term

- Search back in time X days for all unique entries in a field and alert if any new terms appear.

Spike

- Alert when the number of events is higher than a threshold. May be an absolute number of events or percentage larger.

Flatline

- Alert when the number of events is below a threshold for a given time period.

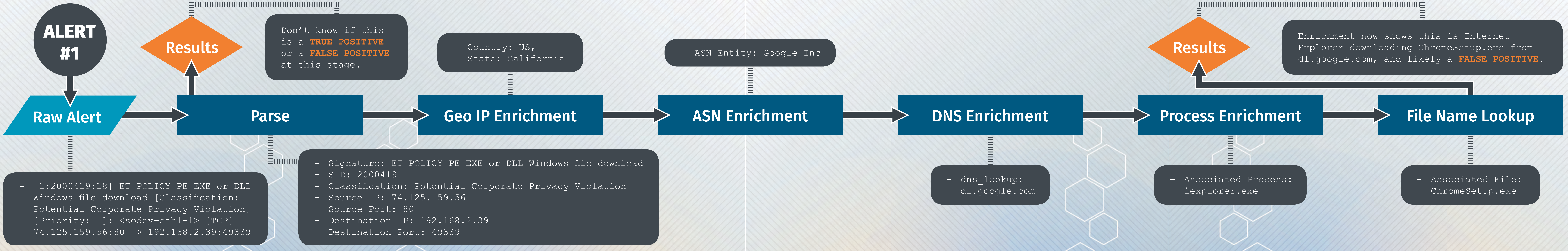
Change

- Alert any time the value of the specific field changes.

SANS

sans.org/SIEM

Log Enrichment



ALERT #1

Raw Alert → Parse → Geo IP Enrichment → ASN Enrichment → DNS Enrichment → Process Enrichment → File Name Lookup

Results

Don’t know if this is a **TRUE POSITIVE** or a **FALSE POSITIVE** at this stage.

```
- [1:2000419:18] ET POLICY PE EXE or DLL
  Windows file download [Classification:
  Potential Corporate Privacy Violation]
  [Priority: 1]: <sodev-eth1-1> {TCP}
  74.125.159.56:80 -> 192.168.2.39:49339
```

```
- Signature: ET POLICY PE EXE or DLL Windows file download
- SID: 2000419
- Classification: Potential Corporate Privacy Violation
- Source IP: 74.125.159.56
- Source Port: 80
- Destination IP: 192.168.2.39
- Destination Port: 49339
```

```
- Country: US,
  State: California
```

```
- ASN Entity: Google Inc
```

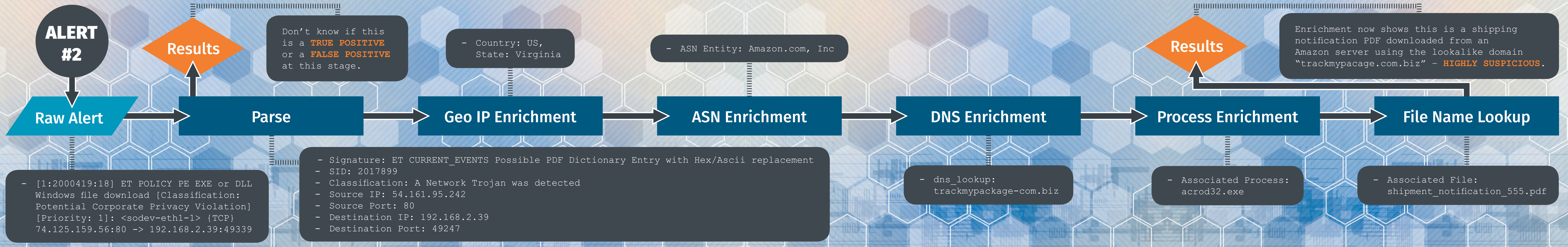
```
- dns_lookup:
  dl.google.com
```

```
- Associated Process:
  iexplorer.exe
```

```
- Associated File:
  ChromeSetup.exe
```

Results

Enrichment now shows this is Internet Explorer downloading ChromeSetup.exe from dl.google.com, and likely a **FALSE POSITIVE**.



ALERT #2

Raw Alert → Parse → Geo IP Enrichment → ASN Enrichment → DNS Enrichment → Process Enrichment → File Name Lookup

Results

Don’t know if this is a **TRUE POSITIVE** or a **FALSE POSITIVE** at this stage.

```
- [1:2000419:18] ET POLICY PE EXE or DLL
  Windows file download [Classification:
  Potential Corporate Privacy Violation]
  [Priority: 1]: <sodev-eth1-1> {TCP}
  74.125.159.56:80 -> 192.168.2.39:49339
```

```
- Signature: ET CURRENT_EVENTS Possible PDF Dictionary Entry with Hex/Ascii replacement
- SID: 2017899
- Classification: A Network Trojan was detected
- Source IP: 54.161.95.242
- Source Port: 80
- Destination IP: 192.168.2.39
- Destination Port: 49247
```

```
- Country: US,
  State: Virginia
```

```
- ASN Entity: Amazon.com, Inc
```

```
- dns_lookup:
  trackmypackage-com.biz
```

```
- Associated Process:
  acrod32.exe
```

```
- Associated File:
  shipment_notification_555.pdf
```

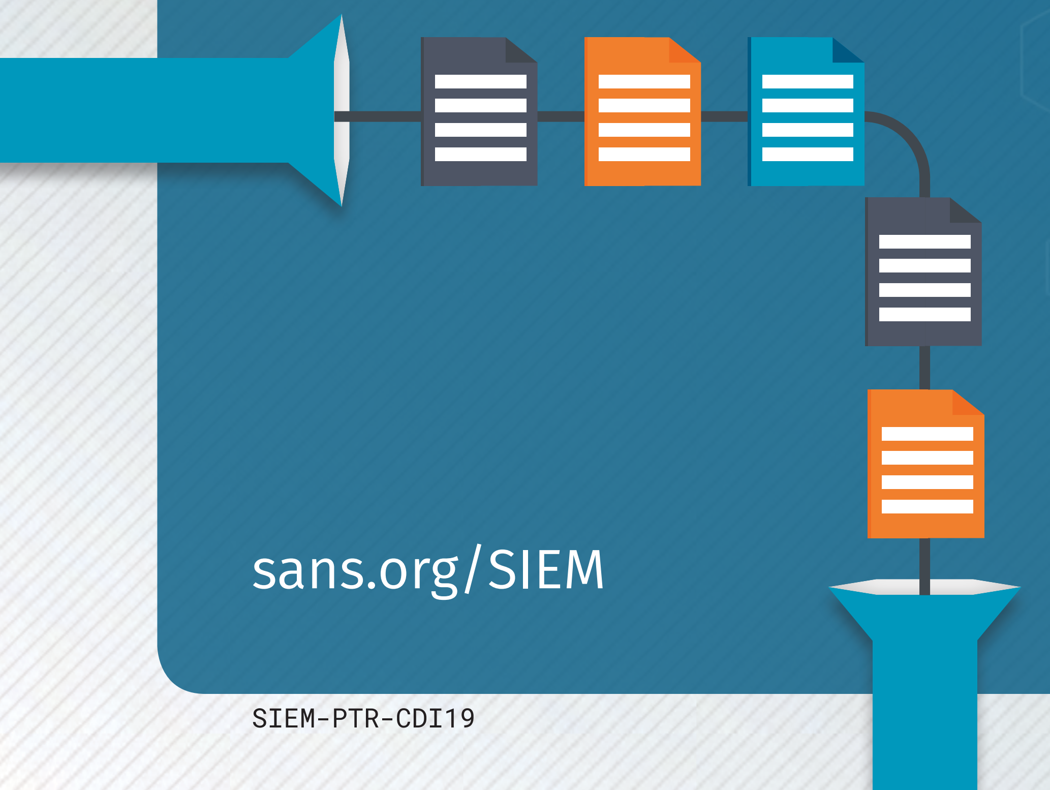
Results

Enrichment now shows this is a shipping notification PDF downloaded from an Amazon server using the lookalike domain “trackmypacage.com.biz” – **HIGHLY SUSPICIOUS**.

SANS

A Log Lifecycle

POSTER



sans.org/SIEM

SANS Training for Security Operations

TIER 1		
SEC401	Security Essentials Bootcamp Style	GSEC
ICS410	ICS/SCADA Security Essentials	GICSP
SEC450	Blue Team Fundamentals – Security Operations and Analysis	
TIER 2		
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC455	SIEM Design & Implementation	
SEC555	SIEM with Tactical Analytics	GCDA
SEC511	Continuous Monitoring & Security Operations	GMON
TIER 3		
SEC503	Intrusion Detection In-Depth	GCED
FOR572	Advanced Network Forensics: Threat Hunting, Analysis & Incident Response	GNFA
FOR610	Reverse-Engineering Malware: Malware Analysis Tools & Techniques	GREM
ICS515	ICS Active Defense & Incident Response	GRID

View a full list of courses at sans.org/training

SIEM Collection Capability & Maturity Progression

	New Deployments	Established Deployments	Mature Deployments
Collection:	Collection of logs from critical assets and hosts that access them	Collection of most at-risk host logs: desktops, servers, and appliances	Full tactical log collection on desktops, servers, appliances, mobile devices, and any other relevant assets
Context Building & Tool Integration:	Building naming standard, basic tagging/categorization	Consistent naming standard, detailed tagging and categorization, some integration with asset DB / vulnerability management data sources, some automation	Using all collected info for anomaly detection (enriched with tagging and asset info), SOAR integration
Detection & Alerting:	High fidelity alert collection, emphasis on rule validation and FP reduction	High fidelity alert queue, established process for lower fidelity alert storage and periodic review	Upgrading of lower fidelity alerts based on context and automation, applied anomaly detection, data science capabilities for beaconing and DGA detection, UEBA
Log Agent Agility:	Automatic, installer pushed (SCCM)	Fully automated deployment and enforcement on all systems	Dynamic agent confirmation based on self-assessed services run on host