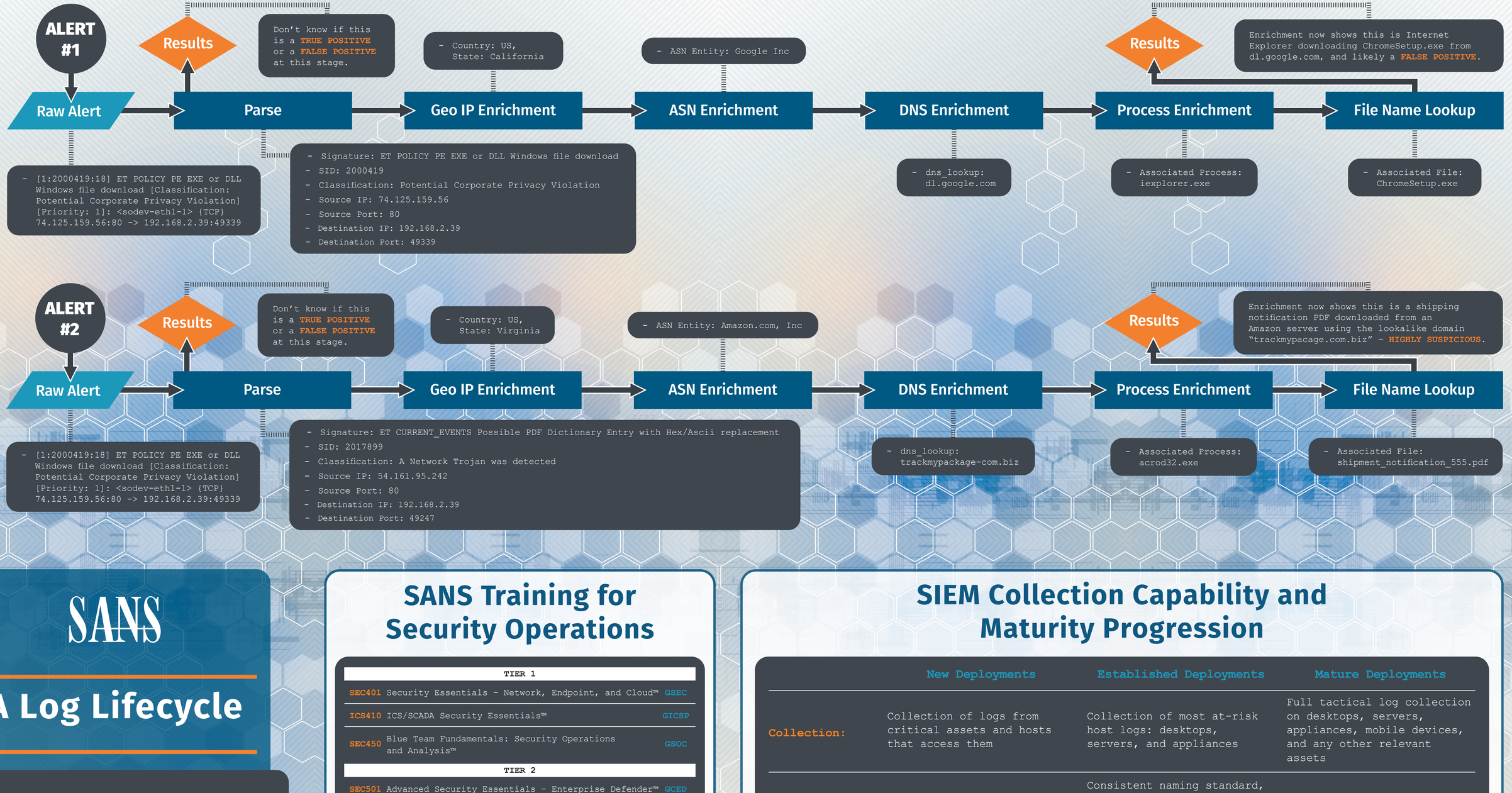
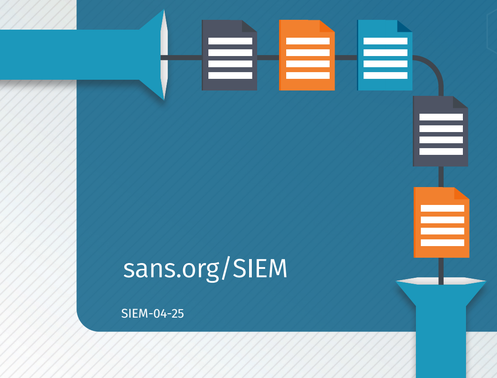
Log Enrichment



SANS

A Log Lifecycle

POSTER



sans.org/SIEM

SIEM-04-25

SANS Training for Security Operations

TIER 1		
SEC401	Security Essentials - Network, Endpoint, and Cloud™	GSEC
ICS410	ICS/SCADA Security Essentials™	GICSP
SEC450	Blue Team Fundamentals: Security Operations and Analysis™	GSOC
TIER 2		
SEC501	Advanced Security Essentials - Enterprise Defender™	GCED
SEC555	Detection Engineering and SIEM Analytics™	GCDA
SEC511	Cybersecurity Engineering: Advanced Threat Detection and Monitoring™	GMON
TIER 3		
SEC503	Network Monitoring and Threat Detection In-Depth™	GCIA
FOR572	Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™	GCIA
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques™	GREM
ICS515	ICS Visibility, Detection, and Response™	GRID
LDR551	Building and Leading Security Operations Centers™	GSOM

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

SIEM Collection Capability and 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 and 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 Ability:	Automatic, installer pushed (SCCM)	Fully automated deployment and enforcement on all systems	Dynamic agent confirmation based on self-assessed services run on host

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
- Third 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

Log Enrichment

See reverse side for detail.

Broker

Storage

Considerations:

- Log volume calculation
- Data lifecycle and 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.

Search

Alert Engines

Alerts

Triage

SANS

sans.org/SIEM