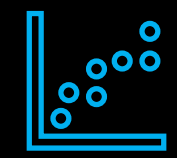




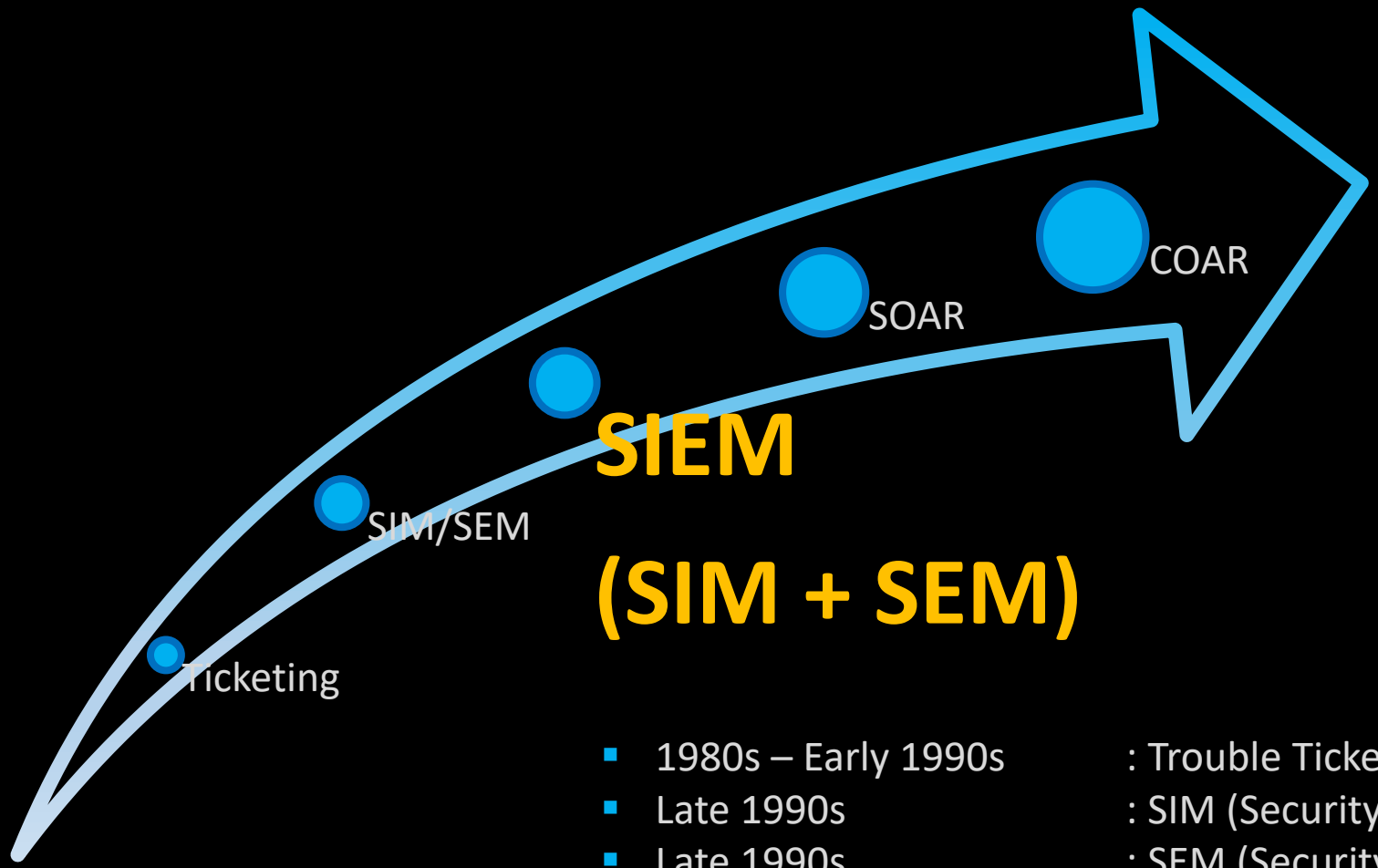

SIEM Internals

Presented by Isuru Tharanga Malawige






EVOLUTION of Security Analytics



- 1980s – Early 1990s : Trouble Ticketing (Help Desk)
- Late 1990s : SIM (Security Information Management) – Historical
- Late 1990s : SEM (Security Event Management) – Real Time
- 2005 – Present : SIEM (Security Information and Event Management)
- 2016 – Present : SOAR (Security Orchestration, Automation and Response)
- 2019 – Present : COAR (Cloud Orchestration, Automation and Response)

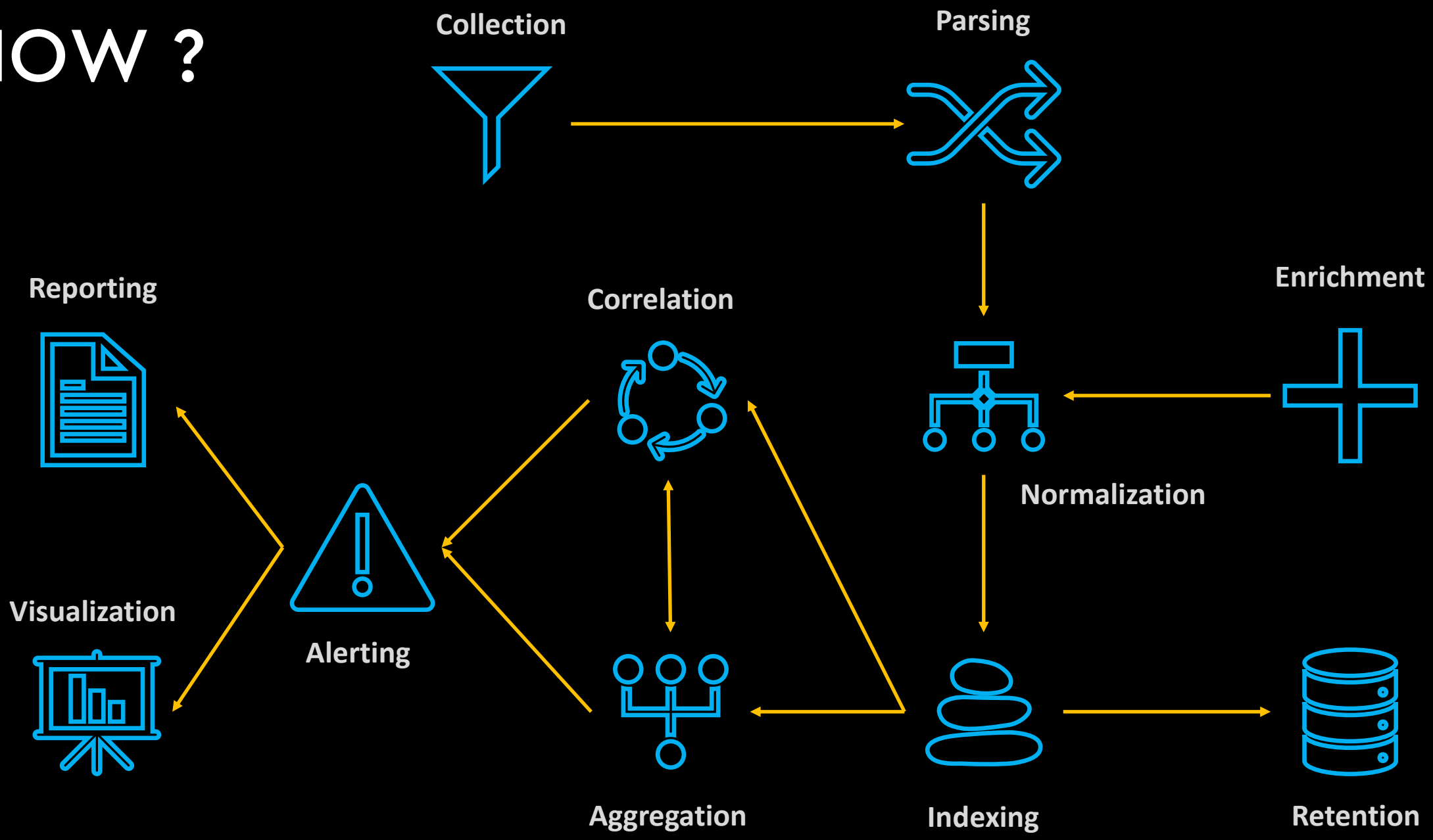
WHY ?

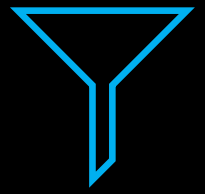
Gartner defines the **Security and Information Event Management (SIEM)** market by the customer's need to **analyze** event data in **real time** for early **detection** of targeted **attacks** and data **breaches**, and to **collect, store, investigate** and **report** on log data for **incident response, forensics** and **regulatory compliance**.

WHAT ?

Gartner defines the **Security and Information Event Management (SIEM)** as a **security technology** that **aggregates** event data produced by **security devices, network infrastructure, systems** and **applications**. The **primary** data source is **log data**, but SIEM technology can also process other forms of data, such as **network telemetry**. Event data is combined with contextual information about **users, assets, threats** and **vulnerabilities**. The data may be **normalized**, so that events, data and contextual information from **disparate sources**. The technology provides **real-time** analysis of events for **security monitoring**, query and **long-range** analytics for **historical** analysis.

HOW ?


Collection
Parsing
Reporting
Correlation
Enrichment
Normalization
Visualization
Alerting
Aggregation
Indexing
Retention



COLLECTION

- Windows
  - Security
  - System
  - Application
  - Sysmon
  - PowerShell
- Linux / Unix
  - Secure
  - Audit
- Web Logs (Access / Error)
  - Apache
  - Nginx
- DB (Audit Trace)
  - MySQL / MariaDB
  - MS-SQL
  - Oracle
- Endpoint Security
  - AV
  - EDR / ATP
- Network/Firewall Devices
  - Logs
    - Traffic
    - IPS
  - SNMP
  - Flow (NetFlow / sFlow / JFlow)
  - Full PCAP (using Network Aggregator)
    - SPAN / Port Mirroring
    - TAP
- Cloud (Instances / Services)
  - Azure (Microsoft)
    - Sentinel
    - o365 Audit
  - AWS (Amazon)
    - CloudTrail
    - CloudWatch
    - GuardDuty/SecurityHub
  - GCP (Google)
    - Audit Logs

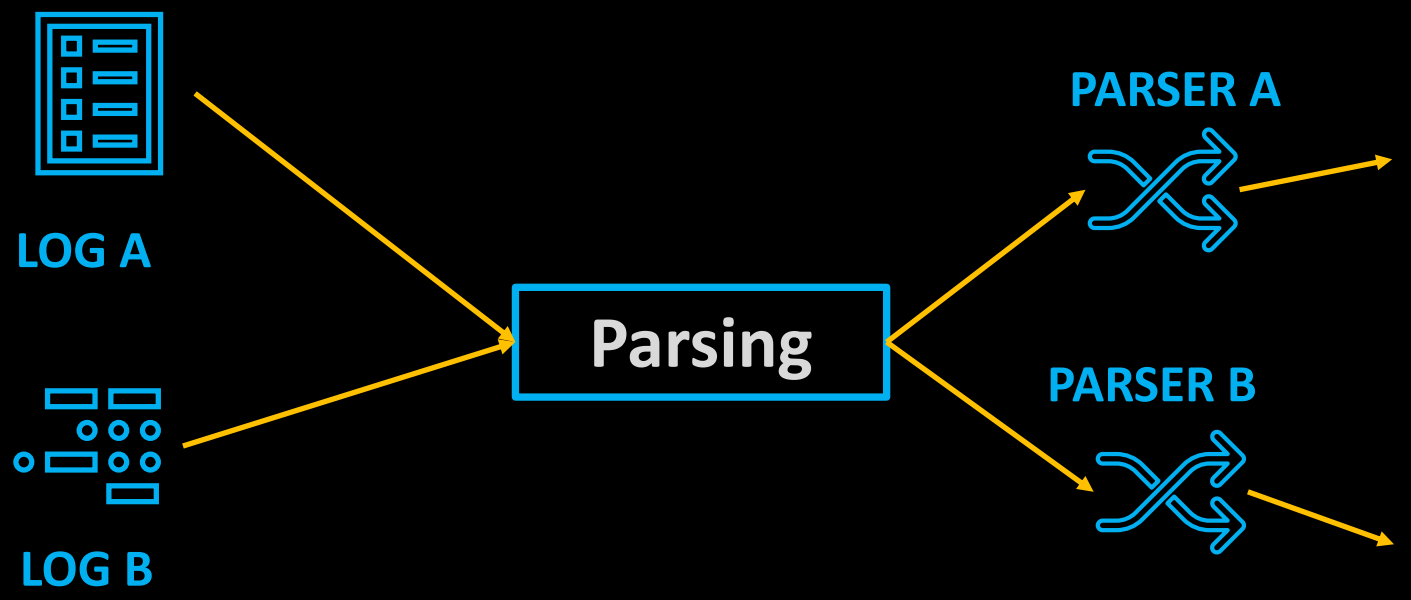
Collection Methods

- Agent
- Syslog
- API
- SNMP

PARSING

Structured Logs (Logs with “Key:Value” Pair)

- **Aug 18 12:27:55 DCE2_EVENT__SMB_NB_LT_SMBHDR|dpt=63927 dst=10.10.130.36 dvchost=COL-DC-FTD-2 proto=TCP spt=64492 src=10.227.40.84 suser=biztalkadmn**

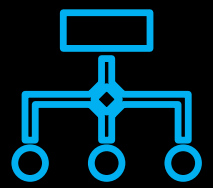


- Source User = biztalkadmn
- Destination IP = 10.10.130.36
- Protocol = TCP
- Source IP = 10.227.40.84
- Destination Port = 63927
- Source Port = 64492

- User = Daniel
- Auth Status = failed
- Source IP Address = 182.54.12.98
- User ID = 34532

Unstructured Logs (Logs only with “Values”)

- **Aug 11 17:22:14 auth0 access denied for userId 34532 Daniel Berman 182.54.12.98**
- **[11/Aug/2020:17:22:14 -0300] 182.54.12.98 authentication failed at login 34532 user Daniel**



NORMALIZATION

LOG A

- Source IP Address
- Destination IP Address
- Application Name
- Destination IP Address

LOG B

- Username
- Event ID
- Login Status
- Reporting Device

LOG C

- URL
- User Agent
- HTTP Status Code
- HTTP Method
- Source IP Address

LOG D

- Source MAC Address
- VLAN ID
- Destination Interface
- Source IP Address
- Destination TCP/UDP Port

Normalization

Reporting Device	SIP	DIP	SPort	Dport	Event ID	VLAN ID	HTTP Status Code	Login Status
A	192.168.34.24	172.19.25.244	34567	80				
C	172.16.15.40			443			200	
D	10.10.146.13			21		20		
B					4624			Success
B					4725			Failure

ENRICHMENT

Reporting Device	SIP	DIP	SPort	Dport	Event ID	VLAN ID	HTTP Status Code	Login Status
D	182.54.12.98	172.19.25.244	34567	80			403	

Geolocation

Enrichment

Threat Intelligence
Ex: IOC (Indicator of Compromise)
Blacklisted IPs
Malware Hashes/Domains

Reporting Device	SIP	DIP	SCountry	Dport	VLAN ID	HTTP Status Code	Login Status	RBL Status
D	182.54.12.98	172.19.25.244	AUS	80		403		**Blacklisted**

THREAT INTELLIGENCE

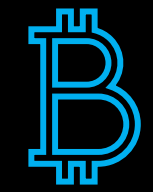
STIX™ TAXII™

Structured Threat Information eXpression, is a standardized language developed by **MITRE** and the **OASIS Cyber Threat Intelligence (CTI) Technical Committee** for describing cyber threat information. It has been adopted as an international standard by various intelligence sharing communities and organizations. It is designed to be shared via TAXII, but can be shared by other means.

Trusted Automated eXchange of Intelligence Information, defines how cyber threat information can be shared via services and message exchanges. It is designed specifically to support STIX information, which it does by defining an API that aligns with common sharing models.

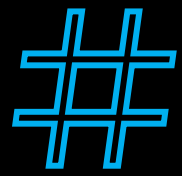
IOCs (Indicators of Compromise)

Malicious IP Addresses



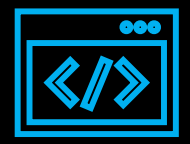
Cryptocurrency Wallet Addresses

Malicious Domains

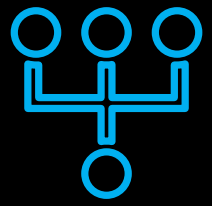


Malware Hashes

Tools / TTPs



Malicious URLs



AGGREGATION

Reporting Device	SIP	DIP	SPort	Dport	Event ID	VLAN ID	HTTP Status Code	Login Status
A	192.168.34.24	172.19.25.244	34567	80			403	
A	192.168.34.24	172.19.25.244	34581	80			403	
A	192.168.34.24	172.19.25.244	34550	80			403	

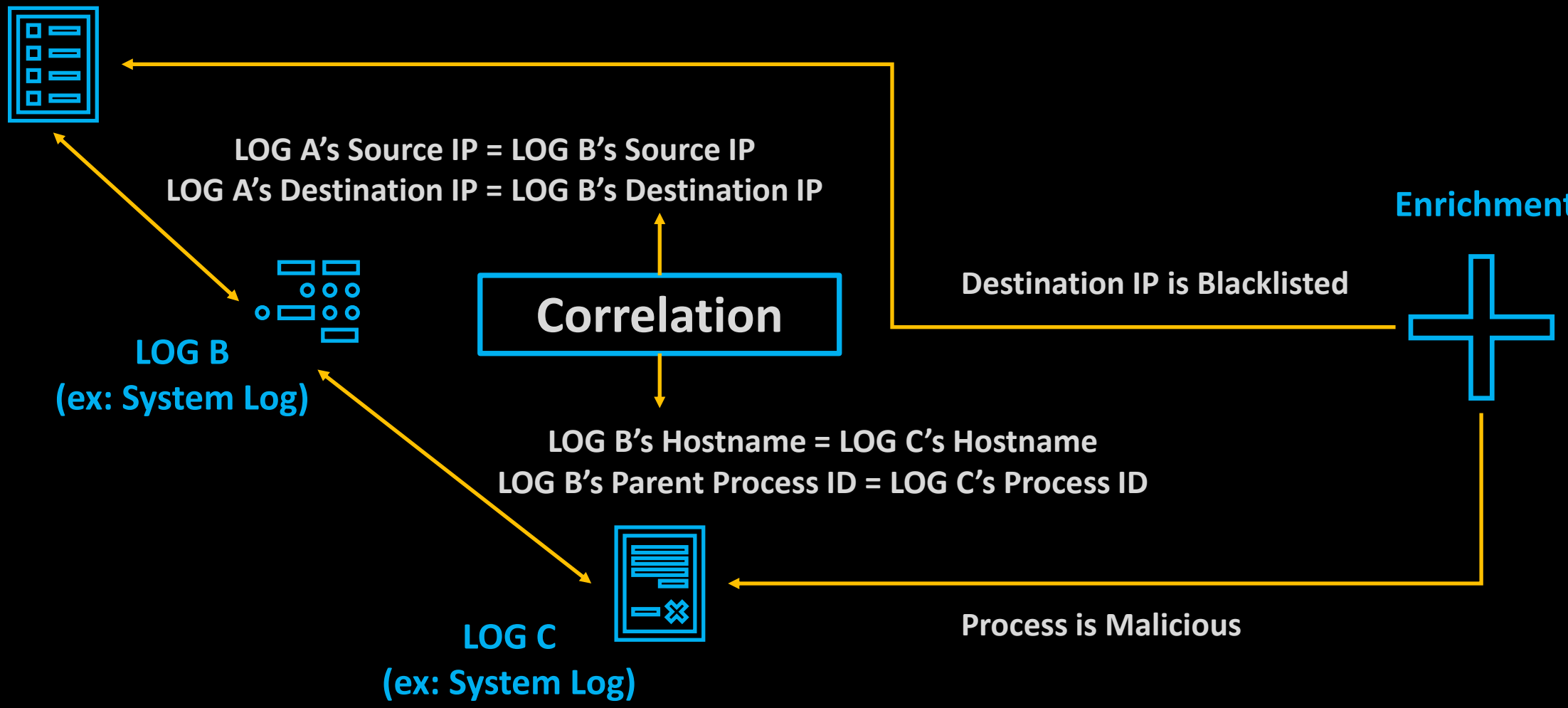
Aggregation

Multiple Unauthorized requests from a specific Host

Reporting Device	SIP	DIP	SPort	Dport	Event ID	VLAN ID	HTTP Status Code	Login Status	Count
A	192.168.34.24	172.19.25.244		80			403		**3**

CORRELATION

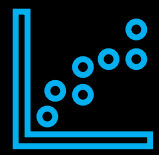
SIEM ALERT: Connection to a Blacklisted IP from a Malicious Process in $hostname



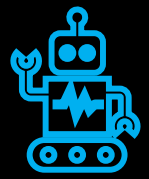
NEXT GEN SIEM ?

User Entity Behavioral Analysis (UEBA)

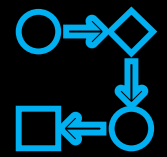
Advanced SIEMs go **beyond** rules and correlations, leveraging **AI** and **ML** techniques to look at **patterns** of **human behavior**. This can help detect insider threats, targeted attacks, and fraud. (deviations from **BASELINE**)



Security Orchestration, Automation and Response (SOAR)



Collect security **threat data** and **alerts** from different sources and enabling **automatic** incident analysis, triage and prioritization using **predefined** standard workflows (**Playbooks**) for **incident response** activities and enforcing **automatic remediations**.



SIEM Market

Enterprise

Open Source

THANK YOU!