Leveraging SIEM

Jeremy Hopwood CISO, Pinnacle Financial Partners

CEO, 5iron – Managed Security Operations

WAIT: WHAT IS A SIEM??

What is a SIEM?

SIEM = **S**ecurity **I**nformation & **E**vent **M**onitoring

Step 1: **Collect Data**, from various logs and sources
(logs from network devices, application & Domain Servers, Security tools, etc)

Step 2: **Aggregate & Normalize** data collection

Step 3: **Analyze** data: Correlate, Enrich, and Detect

Step 4: **Alert**, and pinpoint security events and issues requiring attention

Start with Why? Why most BANKS want SIEM?

(Why some of you think you want a SIEM…..)

1. Because the FFEIC guidelines, auditors, and compliance said they need one.
2. Because they want to automate log reviews, permission reviews, etc. (instead of manual work)
3. Because RISK/Governance said they wanted data analytics, big data capabilities, etc.
4. Because they desire machine learning and behavior analysis
5. Because they want a single source for fighting advanced threats

Why most NEED A SIEM? . . . Leverage

For your information security program & posture

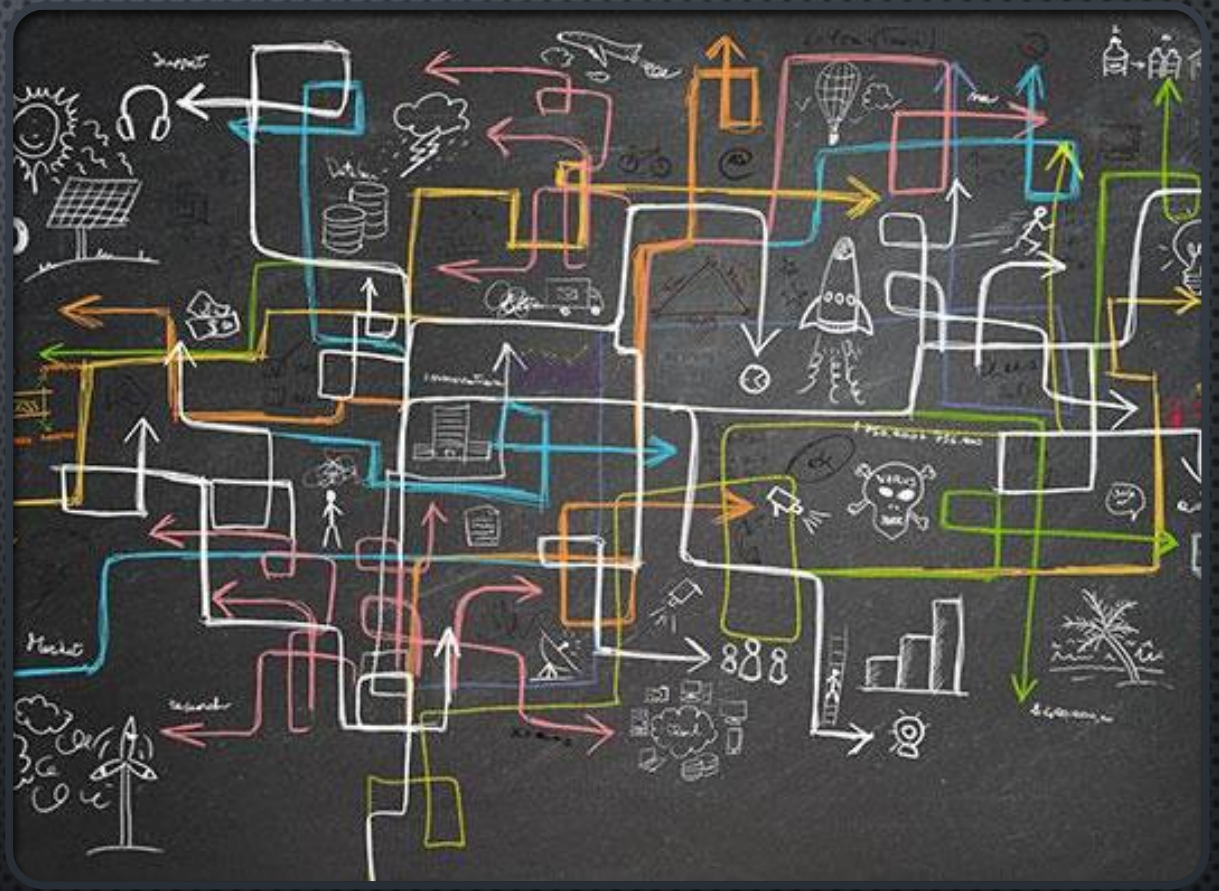
1. **Visibility** — Collect, correlate, and identify threats within your organization.
2. **Focus** — Limited resources can focus on things that matter
   - Needles in haystack vs Haystacks full of needles . . .
3. **Quick Response** — *Reduce response time* and *reduce DWELL* and the unknown
4. **Insight** — Identify areas of weakness, and aide forensic investigations
5. **Compliance** — Exceed regulatory requirements

What a SIEM is Not....

- **An easy button** — a SIEM is complex to deploy and costly to own
- **A singled source solution** — it supports your platform not replace
- **The answer to all your problems** — simply having a SIEM does nothing for your security posture

In Fact . . .

A SIEM implemented or maintained poorly actually **ADDS RISK** to your overall security posture!



The RISK (Real Risk) of having a SIEM:

Underestimated, Poorly Planned or Executed SIEM projects can actually increase your risk.

- **Alert Fatigue**:
- Poorly thought out use cases—or none at all—lead to thousands of alerts
  - Poorly thought out correlation rules —or none at all— lead to maximum low fidelity NOISE (Lots and lots of false positives)

- This Noise leads to alerts being filed and never seen, or simply ignored. This leads to a real threat going ***undetected*** . . . a threat you WERE ACTUALLY ALERTED TO . . .

The RISK (Real Risk) of having a SIEM:

Underestimated, Poorly Planned or Executed SIEM projects can actually increase your risk.

- **Budget issues** — Implementation can drag out for months or even years, unforeseen capital increases for additional compute and storage needed right away. (Did I mention many SIEM charge $$$ by the gig)
- **Production impact** — network impact (depending on-prem vs cloud) [think internet pipe, network fabric, compute architecture) if not taken into consideration.
- **Scale** — Without starting with the end in mind, and developing use cases, scope creep sets in and the “beast” is born. More care, more feeding, more need.

The RISK (Real Risk) of having a SIEM:

Underestimated, Poorly Planned or Executed SIEM projects can actually increase your risk.

- **Beware Blind spots** — false sense of security. Missing segments. Parser not setup properly. Newly added endpoints are missed. Must plan to include future growth to be added/included automatically.

- **Consider Support Impact —** Once the SIEM is running, you need to be ready to both “catch” the output and keep the SIEM in production.
  - Dedicated FTE Subject Matter Expert (SME)
  - Impact to SOC with chasing new alerts.
  - After hours support (7x24x365) the alerts keep coming

HOW TO LEVERAGE SIEM

How To Leverage SIEM: Top 5 Things To Know

1. **Plan architecture, scope, and budget: EYES WIDE OPEN.**

   - Consider Impact to production compute, storage, and bandwidth
   - Log/Data Sources: SIEM is only as good as the data you feed it . . . More data is more data: not better results
     - Baseline all log sources and sizes to understand size
     - Understand corollary between more data/searches to compute, storage, and bandwidth costs
   - Develop a hard timeline for implementation with key milestones and deliverables (regardless if using partner) limit creep
   - Plan for automation - automate as many tasks as possible

How To Leverage SIEM: Top 5 Things To Know

2. Develop Uses Cases: (and owners)

- Should be for security analyst by security analyst. Tell Risk team to get Watson!
- Sample use cases:

Use Case	Example alert(s)
Authentication activities	successful logins, failed logins, etc
Account management	user account creation/deletion, or privilege escalation (domain admin)
Connection activities	denied outbound connection by (geo) location. Attempted FTP connections
Policy-related activities	user authentication from multiple sources. AD password set to never expire
Threat detection	identification of threat indicators. Identification of vulnerable sources
Anomalous behavior	Deleted event logs. Mimikatz credential dump. Windows firewall service was stopped
Operational insight	Data usage by application. Threshold value met. A scheduled task was created
Advanced Correlation & Enrichment	Potential brute force attempt. A remote call procedure was attempted

How To Leverage SIEM: Top 5 Things To Know

3. Care and Feeding: Plan for an Impact to Support

- Make sure you have a trained staff with knowledge of a SIEM product (some developer/scripting skills needed)
  - Make sure that you have more than 1 in case PTO/sick
  - Have a plan for after hours
- Make sure that you have trained information security analysts ready to catch *and* run with the alerts
- Identify granular change in runbooks based on use cases. Triage, afterhours response, and automation
- Maintenance: care & feeding is a serious time commitment: deploying/updating agents, parsing logs (writing new parsers), performing upgrades and updates

Automation is key . . . Partnership is key.

How To Leverage SIEM: Top 5 Things To Know

4. **Build for Enrichment and Context from the start**
    - Threat Intelligence feeds
    - Other value add feeds (API): (Examples)
        - Recordedfuture
        - WHOIS
        - ProcessLibrary
        - Vulnerability scanner

Note: Don’t add confusion through machine learning and behavior analytics until you have the basics

Let's look at an example, and why it matters……

How To Leverage SIEM: Top 5 Things To Know

Enrichment Example:

1. SIEM Alert: you setup an alert to tell you about .EXEs that run on servers in the middle of the night. There is an alert that “maintenanceservice.exe” was just launched on a server.

2. Without context or enrichment, you might scramble the jets. Wake people up. Or at a minimum have people googling to find out what this exe is or does.

- Now, what if you also had this information in the alert:

Name:	**Mozilla Maintenance Service**
Filename:	maintenanceservice.exe
Command:	%ProgramFiles%\Mozilla Maintenance Service\maintenanceservice.exe
Description:	This Windows service is used by FireFox to silently update the program without displaying a Windows User Account Control (UAC) dialog.
Number of times seen in environment:	1

Are you still concerned? Maybe a little – but not at AMBER Alert and launch codes ready. You will now have data to go and precisely dig into it. A quick call to the IT Admin group is in order—to find out WHO loaded FireFox on a production server, and WHY . . .

Context and Enrichment allows for informed decisions.

How To Leverage SIEM: Top 5 Things To Know

5. **Choose the right product.** Make sure your SIEM has:
    - Ability to enrich data
    - Supports automation
        - configuration of data sources, deploy log agents, network extraction, etc
    - Ability to create use-case detection
    - Ability to integrate threat intelligence
    - Scalability
    - Supportability (Ease of use)
    - Maturity

All SIEMs Are Not Created Equal.

EVOLUTION (Think confusion) OF SIEM

- “Traditional” or “Log Centric” vs. “Next Gen”
- **Traditional Product:** Elastic (ELK), LogRhythm, IBM Qradar, Splunk
- **Me-to Product:** Exabeam, Rapid7, Sophos, Fortinet, and everyone else
  - Beware confusion on boundaries (UBA, EUBA, IPS, Threat Hunting, etc)
- **Solution approach:** ATT (Alien Vault), Dell (Secureworks), Regional (Fred’s Schmalien Vault)
- **Partner approach:** Supports your product, your use-case, your goals

SANS “An evaluators guide to NextGen SIEM”
https://www.sans.org/reading-room/whitepapers/logging/paper/38720

Lifeline: Finding the Right Partner

- Even if you get a partner to assist, you need to manage them
- Get expertise: many do what you tell them rather than guide you to best practices
- Beware the big guys: “let me get you to that group who handles that”
- Your priorities (and timeline) are not their priorities
- Beware the magic bullet: a box or service that solves it all.