ALIEN VAULT™

SIEM FOR BEGINNERS

Or: “Everything You Wanted to Know About Log Management
But were Afraid to Ask”

WWW.ALIENVAULT.COM

A ROSE BY ANY OTHER NAME:

SLM/LMS, SIM, SEM,SEC, SIEM

Although the industry has settled on the term ‘SIEM’ as the catch-all term for this type of security software, it evolved from several different (but complementary) technologies before it.

- **LMS - “*Log Management System*” –** a system that collects and store Log Files (from Operating Systems, Applications, etc) from multiple hosts and systems into a single location, allowing centralized access to logs instead of accessing them from each system individually.
- **SLM /SEM**– ***“Security Log/Event Management”*** – an LMS, but marketed towards security analysts instead of system administrators. SEM is about highlighting log entries as more significant to security than others.
- **SIM – “*Security Information Management*”** - an Asset Management system, but with features to incorporate security information too. Hosts may have vulnerability reports listed in their summaries, Intrusion Detection and AntiVirus alerts may be shown mapped to the systems involved.
- **SEC** - **“Security Event Correlation” –** To a particular piece of software, three failed login attempts to the same user account from three different clients, are just three lines in their logfile. To an analyst, that is a peculiar sequence of events worthy of investigation, and Log Correlation (looking for patterns in log files) is a way to raise alerts when these things happen.
- **SIEM – “Security Information and Event Management”** – SIEM is the “All of the Above” option, and as the above technologies become merged into single products, became the generalized term for managing information generated from security controls and infrastructure. We’ll use the term SIEM for the rest of this presentation.

Q: WHAT’S IN THE LOGS? WHAT’S IN THE LOGS?!!

A: **The Information you need to answer “Who’s attacking us today?” and “How did they get access to all our corporate secrets?**

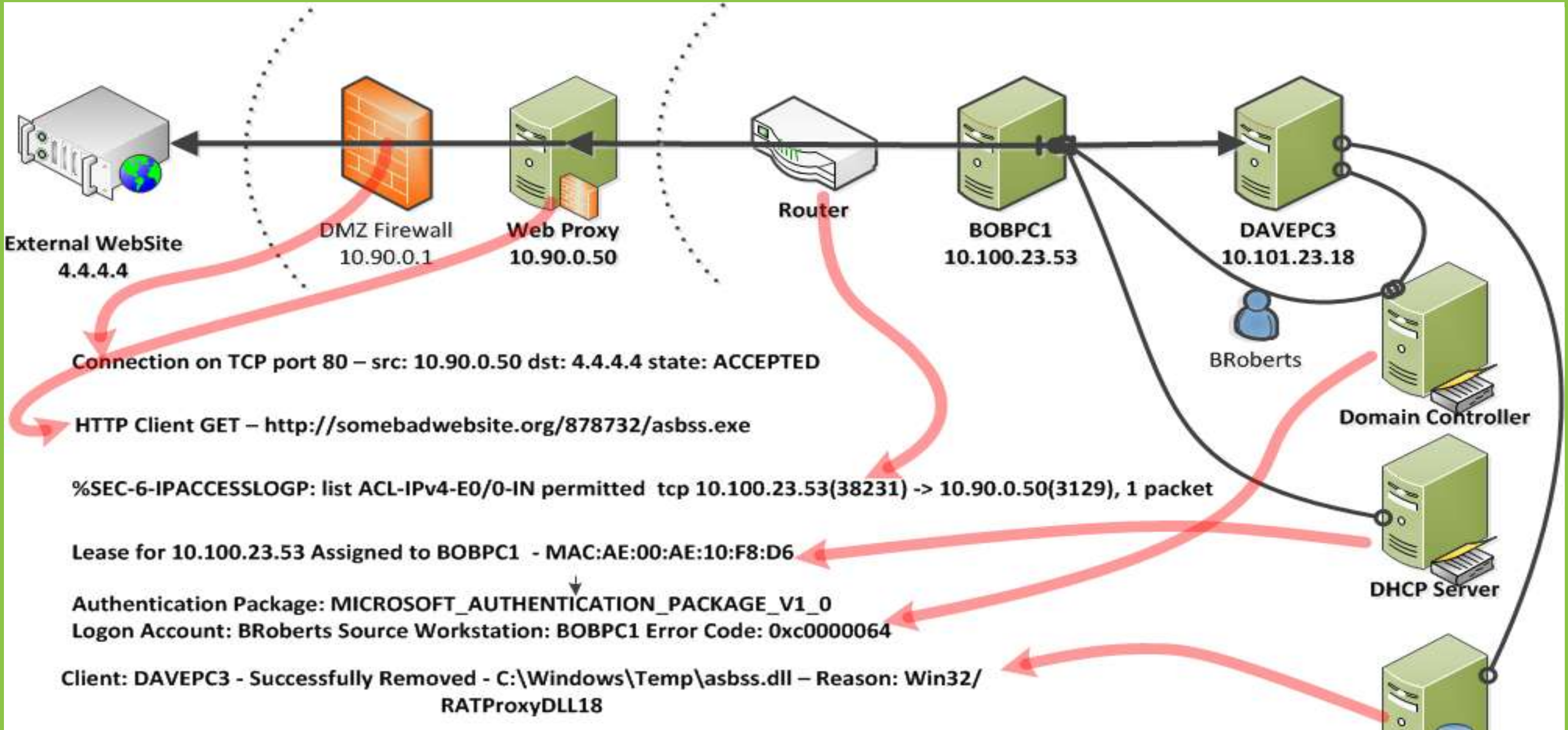
- We may think of Security Controls as containing all the information we need to do security, but often they only contain the things they have detected – there is no ‘before and after the event’ context within them.
- This context is usually vital to separate the false positive from true detection, the actual attack from merely a misconfigured system.
- Successful attacks on computer systems rarely look like real attacks *except in hindsight* – if this were not the case, we could automate **ALL** security defenses without ever needing to employ human analysts.
- Attackers will try to remove and falsify log entries to cover their tracks – having a source of log information that can be trusted is vital to any legal proceeding from computer misuse.

THE BLIND MEN AND THE SECURITY INFORMATION ELEPHANT

- SIEM is about looking at what’s happening on your network through a larger lens than can be provided via any one security control or information source.
  - **Your Intrusion Detection only understands Packets, Protocols and IP Addresses**
  - **Your Endpoint Security sees files, usernames and hosts**
  - **Your Service Logs show user logins, service activity and configuration changes.**
  - **Your Asset Management system sees apps, business processes and owners**
- None of these by themselves, can tell you what is happening to *your business* in terms of securing the continuity of your business processes – but together, they can…

SIEM: A SINGLE VIEW OF YOUR IT SECURITY

- SIEM is essentially, nothing more than a management layer above your existing systems and security controls.
- It connects and unifies the information contained in your existing systems, allowing them to be analyzed and cross-referenced from a single interface.
- SIEM is a perfect example of the ‘Garbage In, Garbage Out’ principle of computing : *SIEM is only as useful as the information you put into it.*
- The more valid information depicting your network, systems and behavior the SIEM has, the more effective it will be in helping you make effective detections, analysis and response in your security operations.



```
Connection on TCP port 80 – src: 10.90.0.50 dst: 4.4.4.4 state: ACCEPTED

HTTP Client GET – http://somebadwebsite.org/878732/asbss.exe

%SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN permitted  tcp 10.100.23.53(38231) -> 10.90.0.50(3129), 1 packet

Lease for 10.100.23.53 Assigned to BOBPC1  - MAC:AE:00:AE:10:F8:D6

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: BRoberts Source Workstation: BOBPC1 Error Code: 0xc0000064

Client: DAVEPC3 - Successfully Removed - C:\Windows\Temp\asbss.dll – Reason: Win32/
RATProxyDLL18
```

"Bob's Machine was compromised by asbss.exe which originated from a malicious website, this malware then used Bobs account to try and infect DAVEPC3, but antivirus caught it. Bob's machine 'BOBPC1' is likely still compromised however. We Should block the malicious domain and sanitize's Bob's workstation, ASAP."

HALF A POUND OF LOGS, A CUP OF ASSET RECORDS….

- Log Collection is the heart and soul of a SIEM – the more log sources that send logs to the SIEM, the more that can be accomplished with the SIEM.
- Logs on their own rarely contain the information needed to understand their contents within the context of your business
- Security Analysts have limited bandwidth to be familiar with every last system that your IT operation depends on
- With only the logs, all an analyst sees is “Connection from Host A to Host B”
- Yet, to the administrator of that system, this becomes “Daily Activity Transfer from Point of Sales to Accounts Receivable”.
- The Analyst *needs* this information to make reasoned assessment of any security alert involving this connection.
- True value of logs is in correlation to get actionable information

SIEM RECIPES

- A list of Ingredients to have a good SIEM Deployment

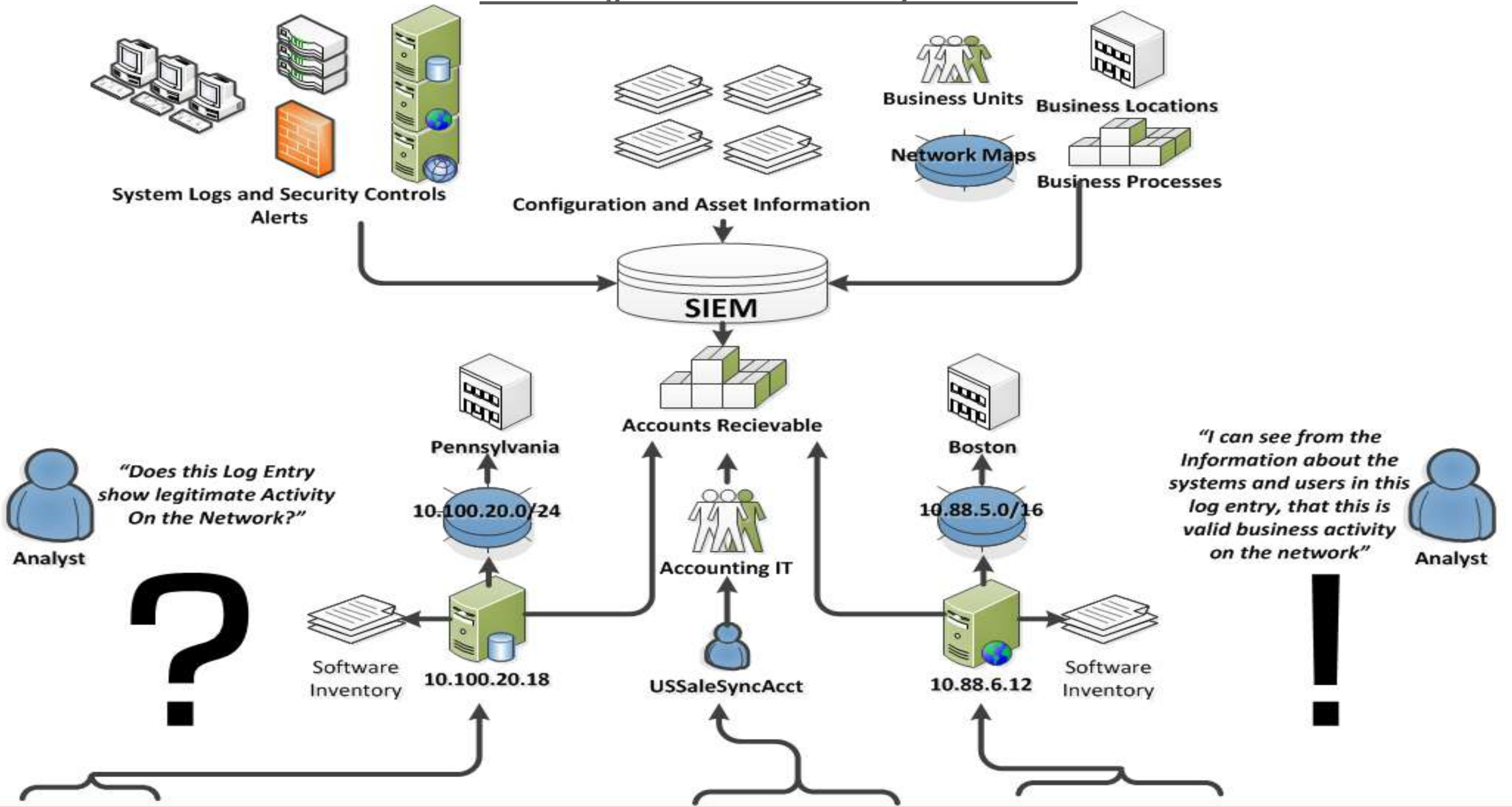
LOGS AND ALERTS:

- Security Controls
  - Intrusion Detection
  - Endpoint Security (Antivirus, etc)
  - Data Loss Prevention
  - VPN Concentrators
  - Web Filters
  - Honeypots
  - Firewalls
- Infrastructure
  - Routers
  - Switches
  - Domain Controllers
  - Wireless Access Points
  - Application Servers
  - Databases
  - Intranet Applications

KNOWLEDGE:

- Infrastructure Information
  - Configuration
  - Locations
  - Owners
  - Network Maps
  - Vulnerability Reports
  - Software Inventory
- Business Information
  - Business Process Mappings
  - Points of Contact
  - Partner Information

How a Log File is Generated in your Network


System Logs and Security Controls Alerts
Configuration and Asset Information
Business Units
Business Locations
Network Maps
Business Processes
SIEM
Accounts Recievable
Pennsylvania
Boston
"Does this Log Entry show legitimate Activity On the Network?"
Analyst
10.100.20.0/24
Accounting IT
10.88.5.0/16
"I can see from the Information about the systems and users in this log entry, that this is valid business activity on the network"
Analyst
?
!
Software Inventory
10.100.20.18
USSaleSyncAcct
10.88.6.12
Software Inventory

```
10.100.20.18 Initiated Database Copy using  credentials ‘ USSalesSyncAcct’ to remote Host 10.88.6.12 – Status Code 0x44F8
```

BEHOLD, THE POWER OF CORRELATION

- Correlation is the process of matching events from systems (hosts, network devices, security controls, anything that sends logs to the SIEM)
- Events from different sources can be combined and compared against each other to identify patterns of behavior invisible to individual devices…
- They can also be matched against the information specific to *your* business.
- Correlation allows you to automate detection for the things that should not occur on *your* network.

THE BEAUTY OF LOG CORRELATION

- Log Correlation is the difference between:

```
"14:10 7/4/20110 User BRoberts Successful Auth to 10.100.52.105 from
10.10.8.22"
```

and…

“An Account belonging to Marketing connected to an Engineering System from an office desktop, on a day when nobody should be in the office”

SLOW COOK FOR 8 HOURS, SERVE TO HUNGRY ANALYSTS….

- Your Network generates vast amounts of log data – a fortune 500 enterprise's infrastructure can generate 10 Terabytes of plain-text log data per month, without breaking a sweat.
- You can't hire enough people to read every line of those logs looking for bad stuff. I'm serious, don't even try this. Even if you succeeded, they'd be so bored they'd never actually spot anything even if it was right in front of their face.. Which it would be.
- Log Correlation lets you locate the interesting places in your logs – that's where the analysts start investigating from…
- ..And they're going to find pieces of information that lead to other pieces of information as the trail of evidence warms up..
- Being able to search through the rest of those logs for that one thing they suspect resides there, is one of the other key functions of a SIEM….
- It's a good thing that a SIEM is fundamentally a…..

…..GIANT DATABASE OF LOGS.

- It would be amazingly useful if every operating system and every application in the world, recorded their log events in the same format – they don't. Most logs are written to be readable by humans, not computers.
- That makes using regular search tools over logs from different sources… a little difficult.
- These two logs say the same thing to a human being, but are very different from the machine's point of view.

```
“User Broberts Successfully Authenticated to 10.100.52.105 from client 10.10.8.22”
“100.100.52.105 New Client Connection 10.10.8.22 on account: Broberts: Success”
```

- Long story short – we're going to need to break down every known log message out there, into a normalized format.

```
“User [USERNAME] [STATUS] Authenticated to [DESTIP] from client [SOURCEIP]”
“100.100.52.105 New Client Connection 10.10.8.22 on account: Broberts: Success”
```

- So when you see a SIEM Product that talks about “how many devices it supports” – it's talking about how many devices it can parse the logs from.

SEARCHES, PIVOTING, AND CROSS-CORRELATION

- Breaking those log entries down into their components – *normalizing* them, is what allows us to search across logs from multiple devices, and correlate events between them.

- Once we've normalized logs into a database table, we can do database style searches, such as :

  "Show [All Logs] From [All Devices] from the [last two weeks], where the [username] is [Broberts]"

- This is what allows us to do automated correlation as well, matching fields between log events, across time periods, across device types.

  "If A single Host fails to log in to three separate servers using the same credentials, within a 6-second time window, raise an alert"

- Just as with any database, event normalization allows the creation of report summarizations of our log information

  "What User Accounts have accessed the highest number of distinct hosts in the last month?"

  "What Subnet generate the highest number of failed login attempts per day, averaged out over 6 months?"

BUT WAIT, THERE’S MORE!

- So you’ve now seen that SIEM is a recording device for the systems that form your information infrastructure.

- SIEM allows you to give analysts access to information from these systems, without giving them access to the systems themselves.

- Event Correlation allows you to encode security knowledge into automated searches across events and asset information to alert on things happening within your infrastructure, and create a starting point for human analysis into a sea of log data.

- But, to keep up with today’s threat landscape you need more that just SIEM – you need relevant data, a unified approach and integrated threat intelligence to truly get a holistic view of your security posture.

- *OBLIGATORY PRODUCT PITCH TIME:* AlienVault USM and OSSIM (Open-source version), are designed to include many data sources as part of core product and provides the threat intelligence to stay ahead.

MANY POINT SOLUTIONS…INTEGRATION ANYONE?

OR

AlienVault USM

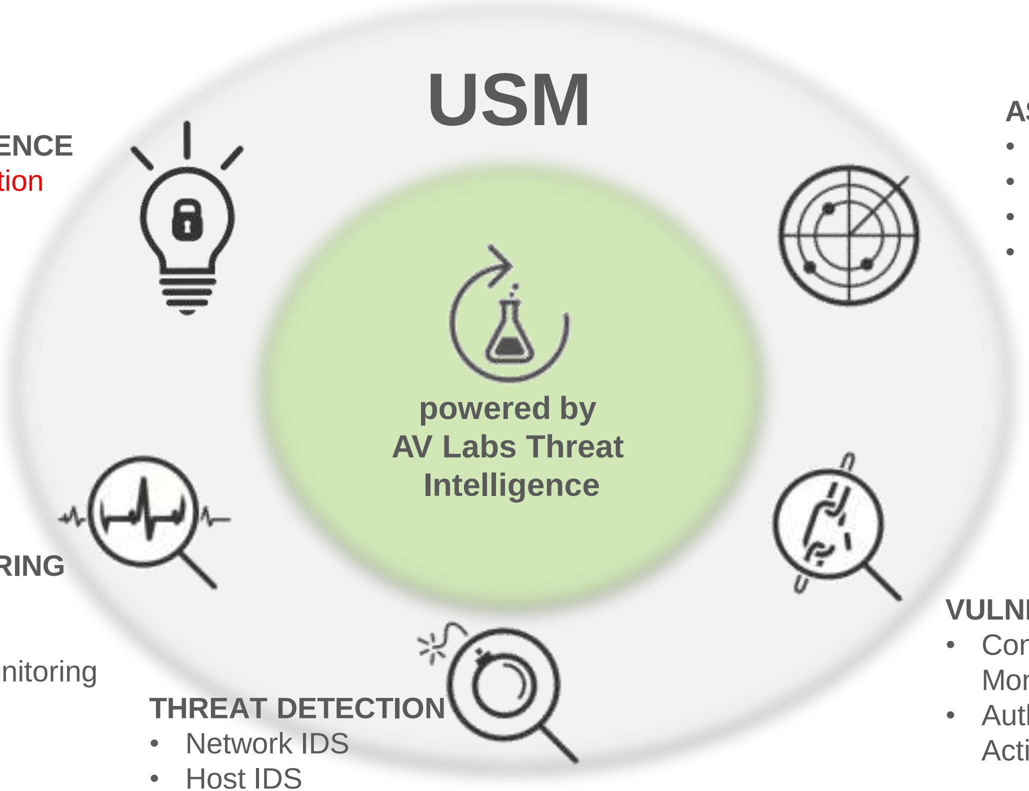
ALIENVAULT USM BRINGS IT ALL TOGETHER

SECURITY INTELLIGENCE

- SIEM Event Correlation
- Incident Response

ASSET DISCOVERY

- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Host-based Software Inventory



BEHAVIORAL MONITORING

- Log Collection
- Netflow Analysis
- Service Availability Monitoring

THREAT DETECTION

- Network IDS
- Host IDS
- Wireless IDS
- File Integrity Monitoring

VULNERABILITY ASSESSMENT

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning

AlienVault USM starts at $3600

Features:	AlienVault USM	Traditional SIEM
Log Management	✔	✔
Event Management	✔	✔
Event Correlation	✔	✔
Reporting	✔	✔
Asset Discovery	✔	$$ 3rd-party product that requires integration
Network IDS	✔	$$ 3rd-party product that requires integration
Host IDS	✔	$$ 3rd-party product that requires integration
Wireless IDS	✔	$$ 3rd-party product that requires integration
NetFlow	✔	$$ 3rd-party product that requires integration
Full Packet Capture	✔	$$ 3rd-party product that requires integration
Vulnerability Assessment	✔	$$ 3rd-party product that requires integration
Continuous Threat Intelligence	✔	Not Available
Unified Console for Security monitoring technologies	✔	Not Available

RECOMMENDED NEXT STEPS:

Play, share, enjoy!

- Learn more about our commercial offering
  - Try AlienVault USM, free for 30 days
  - Join us for a LIVE Demo (hosted every Thursday)
- Or try our Open Source version
  - Download OSSIM
- Join the Open Threat Exchange (OTX) , the world’s largest crowd-sourced threat sharing repository.