WHAT IS LOG CORRELATION?

Understanding the most powerful feature of SIEM

WWW.ALIENVAULT.COM

IT’S ALWAYS IN THE LOGS….

- 84% of Organizations that had their security breached in 2011, had evidence of the breach in their log files.
- Most systems’ log files don’t contain entries that say “Help! Help! I’m being attacked!” however.
- Yet when a skilled human reads those log files, they can show the sequence of events that indicates the machine being compromised – *especially* when they cross-reference them against logs from other systems..

…EXCEPT WHEN IT ISN'T IN THE LOGS….

- Logs vary greatly from system to system
  - With rare exceptions, there are few standards that software and systems adhere to for what is logged and to what level of detail.
  - Some logs are in plain language, others contain cryptic status codes.
  - System logs don't say "Help! Help! I'm being broken into with a compromised account!" – they say "Successful Login from Authenticated User"
  - System logs by themselves are dependent on human analysis to make interpretations from.

THE BLIND MEN AND THE ELEPHANT

- Each system and control on a network has a particular type of tunnel vision – it sees the world through a particular lens.
- While a Network Intrusion Detection systems sees packets and streams, an Application log sees sessions, users and requests – each is logging the same activity, but from a different viewpoint.
- Many systems are entirely ignorant of the business processes they serve – It is possible that a web application sees “Joe from Accounting”, the underlying webserver only sees “jdobson1”

FIXED POINTS IN TIME.

- Since there are few standards in what information is logged, and to what detail, most logs describe events as discrete points in time.
  - “User jdobson1 disconnected”

    is encountered far more often than
  - “User jdobson1 disconnected after 3hrs 15mins from a session originating from 192.168.1.10”
- All too often, human analysis is required to extract the things that are inferred within log data, not stated outright.

TIME AND SPACE

- What may be described in a single sentence in natural language, often requires many log entries across a period of time and from multiple sources.
- “Joe Dobson logged into the time tracking system and updated five people’s account information” could require a hundred log entries to demonstrate it happened.
- This sequence of events however, can be described too. For example, first finding Joe’s session ID in the web application, and then matching that session ID to database change logs in the following time period, correlating them together into a single section of logs.

HIGHLY LOGICAL, CAPTAIN

- Log correlation is about constructing rules that look for sequences and patterns in log events that are not visible in the individual log sources.
- They describe analysis patterns that would require human interpretation otherwise, tied together by Logical Operators.
  - “IF a new user IS created on the domain AND a new change control ticket IS NOT created in the change control database”

I’D LIKE A SECOND OPINION

- No Security Control is perfect.
- We talk of “False Positives” and “Tuning” of security controls.
- When something *actually* happens however, there will usually be more than one record of it happening.
  - If Event B only happens if Event A occurs first, and we see Event A followed by Event B, we know that Event A actually did occur”
  - “Web Proxy detected possible Malware from a site was downloaded to a host. Antivirus on that Host reports malware was detected and removed” – We can absolutely confirm that this site is serving malware.

EVERYBODY IS DIFFERENT, EVERYBODY IS THE SAME

- Log correlation allows for the creation of alerts that represent what is important to *your* business processes and security risks.
- Done correctly, Log Correlation is the difference between reacting to:
  - “POSSIBLE-EXPLOIT: mssql improperly formed packet headers”

    Or

  - “User In Accounting Department seen logging into Financial Database from a workstation in Customer Support Department”

THE SHORT VERSION

- Log correlation monitors incoming logs for logical sequences, patterns and values to identify events that are invisible to individual systems.
- They can perform analysis that would otherwise be done by repetitive human analysis.
- They can identify things happening that are unusual for *your* business processes.
- By comparing events from multiple sources they can provide more context and certainty as to what is happening on your infrastructure.
- They can prioritize investigation and analysis work by prefiltering log events into meaningful alerts.

THE POWER OF CORRELATION

- Compare events from multiple sources to track users and processes across systems.
- Track events across time periods to look for sequences of activity that should not normally occur
- Encode human knowledge about what it not normal for a system, or indicates a probably attack, into automatic monitoring.

BUT WAIT, THERE'S MORE!

- Sure, Log Correlation is the most powerful feature in SIEM

- 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.

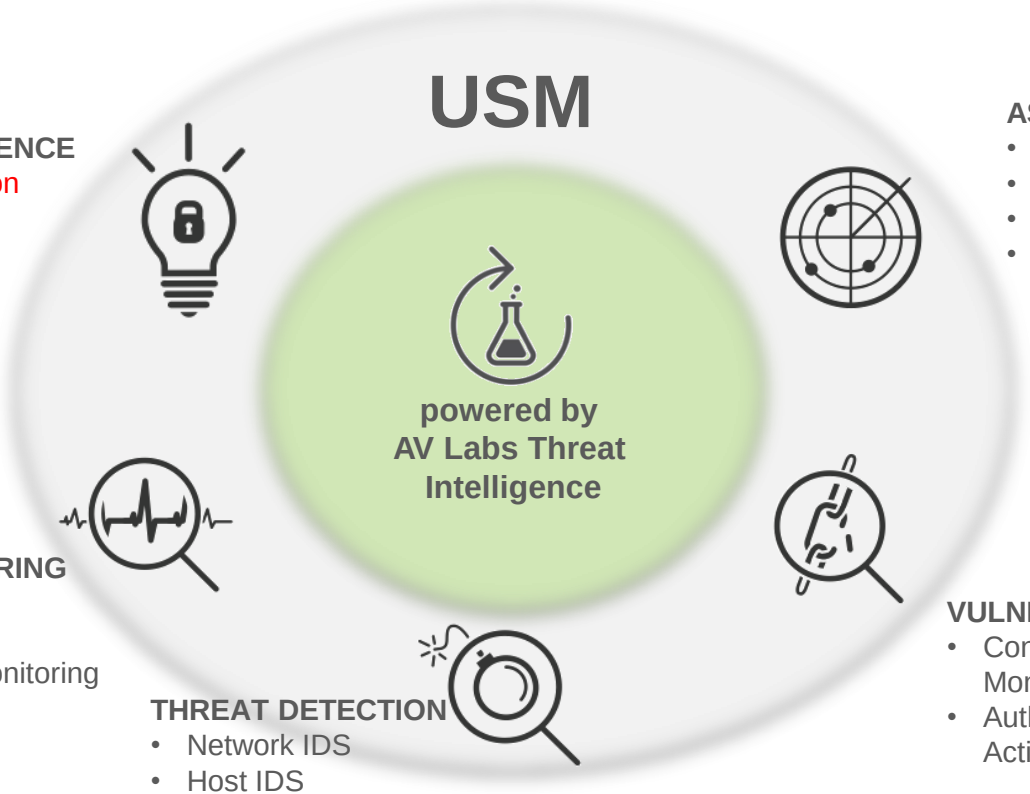
- *OBLIGATORY PRODUCT PITCH TIME:* AlienVault USM and OSSIM (Open-source version), are designed to include many data sources as part of core product and provides the threat intelligence to stay ahead.

MANY POINT SOLUTIONS…INTEGRATION ANYONE?

OR

AlienVault USM

ALIENVAULT USM BRINGS IT ALL TOGETHER



SECURITY INTELLIGENCE
- SIEM Log 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	✔	✔
Log 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.