SIEM 101:

Get a Clue About IT Security Analysis

Joe Schreiber, Solutions Architect
Garrett Gross, Sr. Technical PMM

ALIEN VAULT

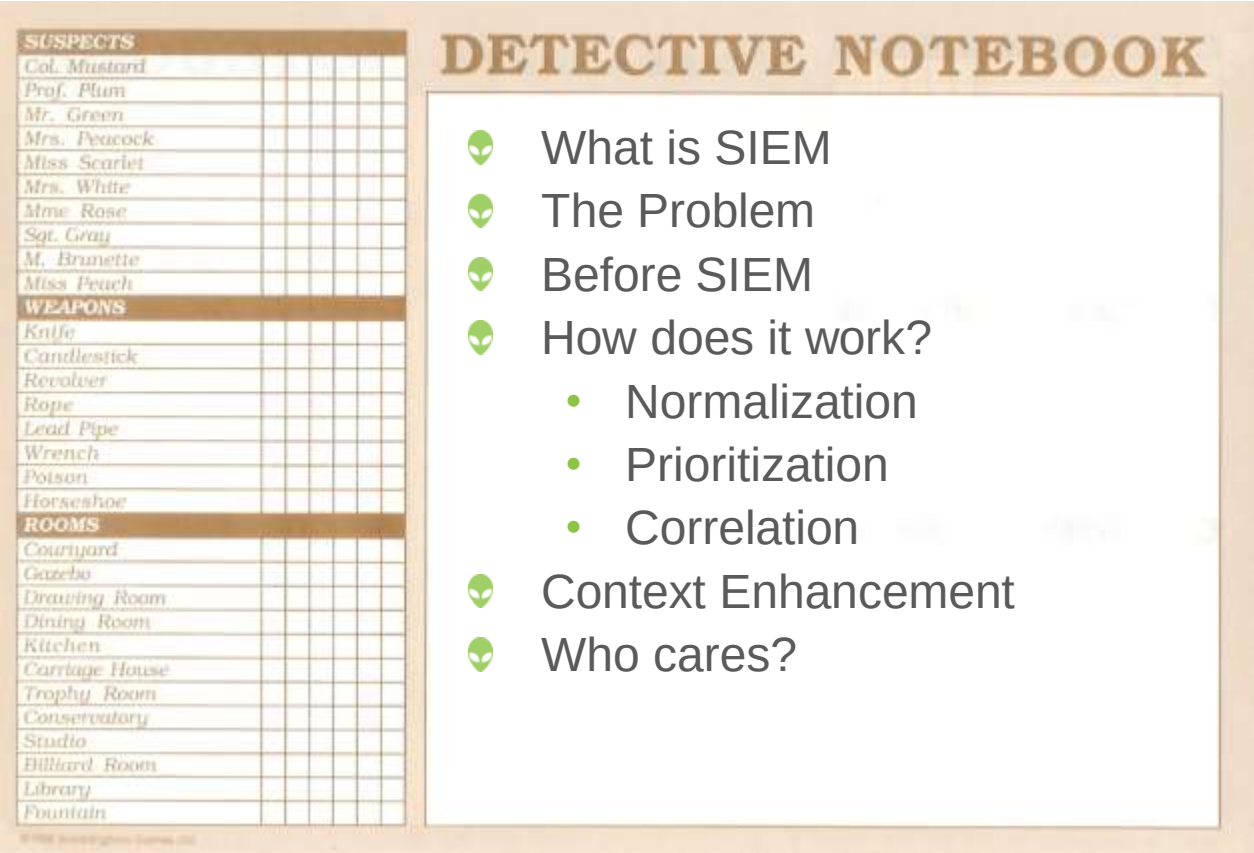
About AlienVault

AlienVault has unified the security products, intelligence and community essential for mid-sized businesses to defend against today's modern threats

Your Presenter…

- Who's Joe?
  - Solutions Architect @ AlienVault
  - SIEM Enthusiast
  - Former SOC Manager/Analyst/Programmer w/ AT&T Managed Security Services
- Resources
  - Blog Posts
    - Open Source Intrusion Detection Tools: A Quick Overview
    - MSSP – The New Acceptance
  - Webinars
    - Data Sources, Policies, and more…
  - Webinar Series: Practitioners Guide
    - Practitioners Guide to SOC
    - The One-Man SOC
    - SIEM 101 *-- in progress*

****Help Joe select his next webinar topic!** Tweet: @pkt_inspector



DETECTIVE NOTEBOOK

- What is SIEM
- The Problem
- Before SIEM
- How does it work?
  - Normalization
  - Prioritization
  - Correlation
- Context Enhancement
- Who cares?

@AlienVault

WHAT IS SIEM?

Acronyms are Fun!

Fancy lettering makes it look cool

Security

Information

Event

Management

But what about?

- SEM – Security Event Management
- SIM – Security Information Management
- SIEM – Security Incident & Event Management
- Log Management
- ESM
- Central Loghost
- Indexing
- ??Big Data??

Why I Like SIEM

Automation

Security

THE PROBLEM FOR SIEM

The Beginning

Not much happening here….

The Interwebs

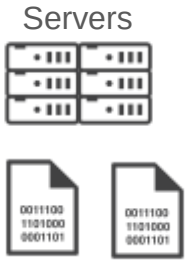
Crash Override

Administrator

Add Some Servers

Still not really interesting…

The Interwebs



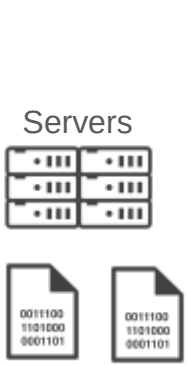
Crash Override

Administrator

Add Some Threats

Starting to get interesting…

The Interwebs



Crash Override

Administrator

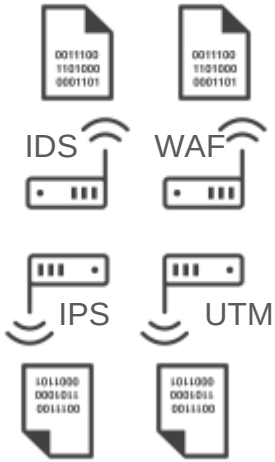
Maybe You Are Here?

Oh Noze!

The Interwebs

Crash Override

Servers



IDS

WAF

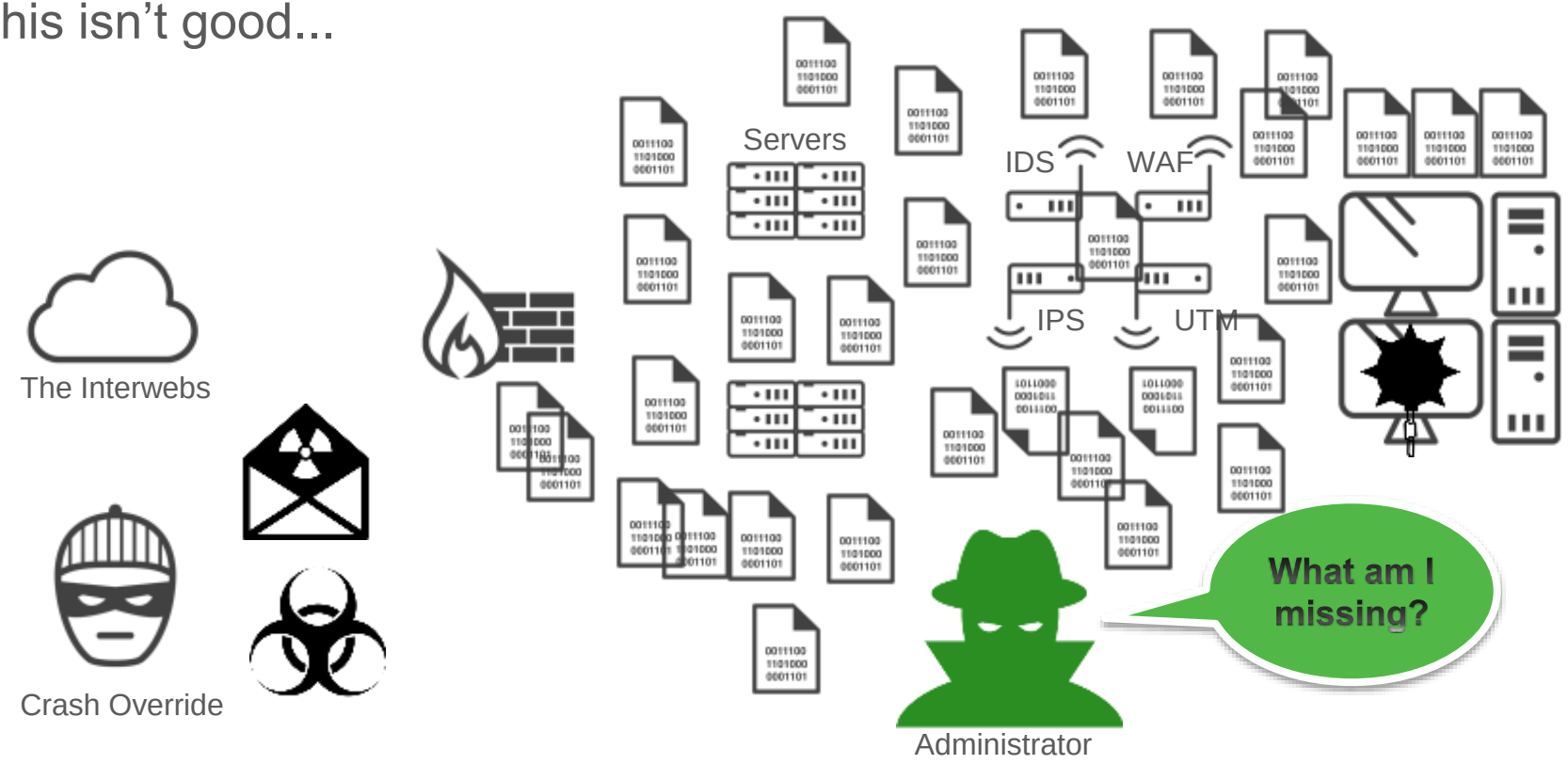
IPS

UTM

Administrator

Where You Really Are

This isn't good...



BEFORE SIEM

What they did back in the ol’ days

- Logs? What are those?
- Oh Logs? Yeah we just keep those on the server.
- Logs? We send those to a central server.
- Why are we storing these log?
- Maybe we search the logs?
- Now I’m bored.

We've come a long way

The Evolution

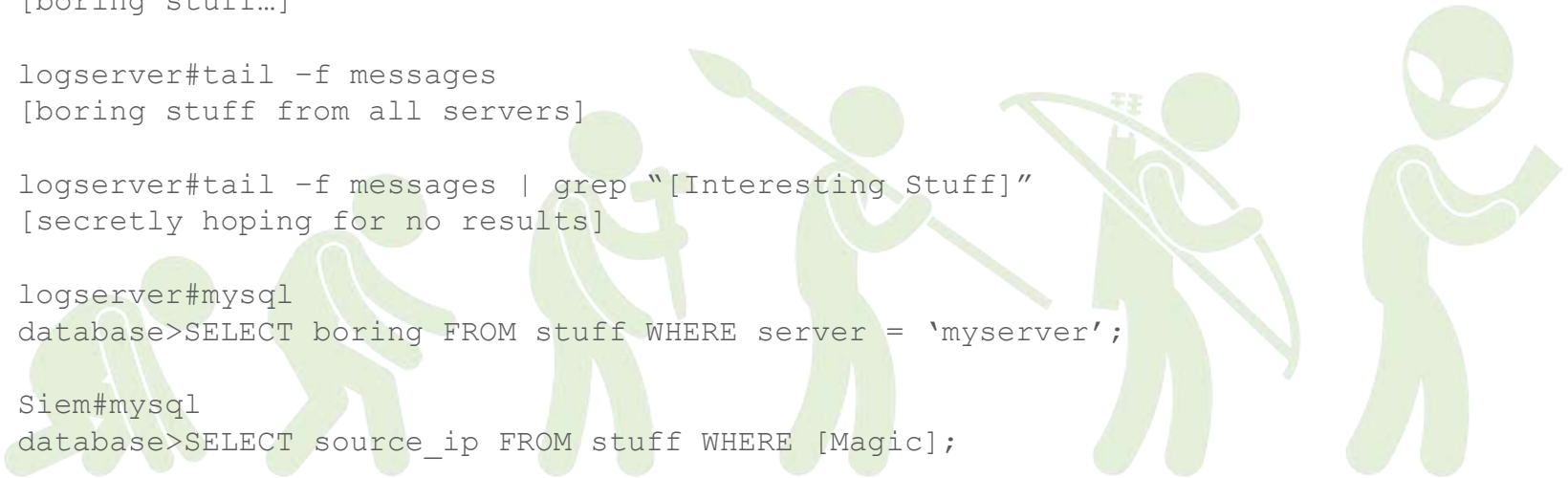
```
server#tail –f messages
[boring stuff…]

logserver#tail –f messages
[boring stuff from all servers]

logserver#tail –f messages | grep "[Interesting Stuff]"
[secretly hoping for no results]

logserver#mysql
database>SELECT boring FROM stuff WHERE server = 'myserver';

Siem#mysql
database>SELECT source_ip FROM stuff WHERE [Magic];
```



All Search and No Intelligence

Why SIEM?

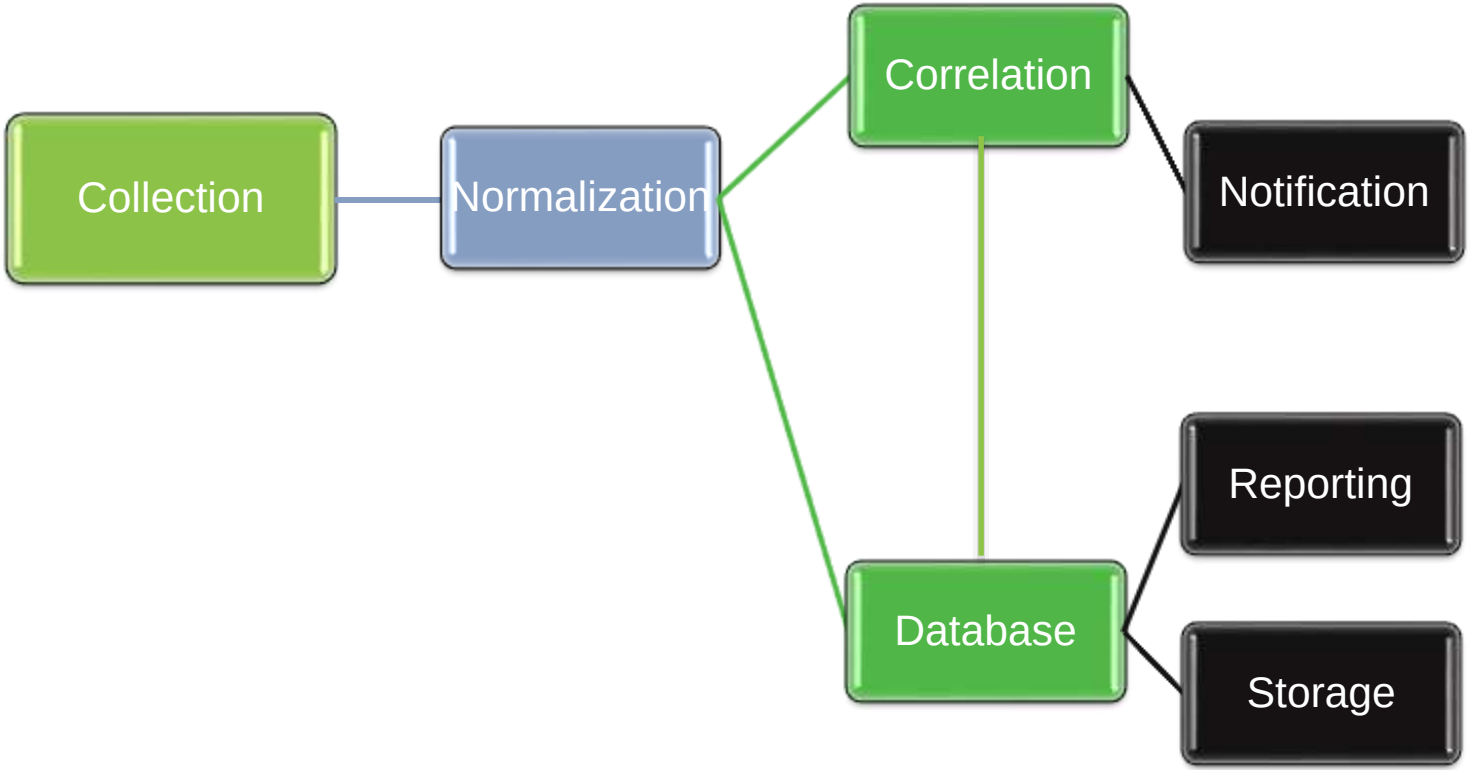
- You can do more than just write logs to disk
- Patterns of events are as important as a single event
- Search can not easily answer
  - What is this server?
  - How important is this server?
  - Why is this data being exchanged?
  - Who is responsible for this server?

How SIEM Works

It’s Magic!

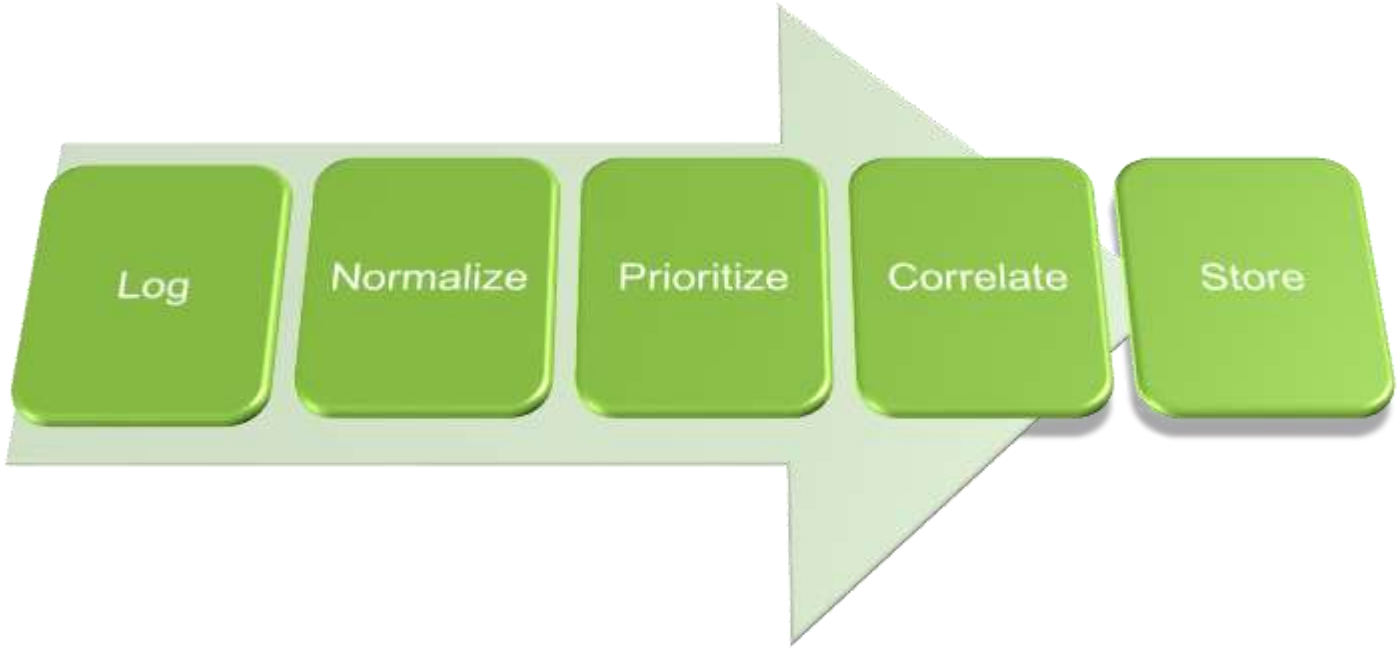
ARCHITECTURE

The Building Blocks



Log Lifecycle

Log goes in…Event comes out



NORMALIZATION

Normalization

Making logs useful

- Logs are usually unstructured pieces of information
- Normalization adds structure
- Databases are structured
- There are different methods of normalization
- The output is the same no matter the method

Turning Chaos Into Order

Start

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

End

Date	10/10/2000 13:55:36
Source IP	127.0.0.1
Username	frank
URL	/apache_pb.gif
Status	200
Bytes	2326

Aren't All Logs Just The Same?

May 21 20:22:28 slacker sshd[21487]: Failed password for root from 192.168.20.10 port 1045 ssh2	source_IP: 192.168.200.10 source_port: 1045 user: root
May 21 20:22:44 slacker proftpd[25557] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]):2023 USER root (Login failed): Incorrect password.	source_IP: 192.168.200.10 source_port: 2023 user: root
Account For Which Logon Failed: Security ID: NULL SID Account Name: root Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Network Information: Workstation Name: WIN-R9H529RIO4Y Source Network Address: 192.168.20.10 Source Port: 53176 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM	source_IP: 192.168.200.10 source_port: 53176 user: root

PRIORITIZATION

Prioritization

What's more important?

- One of the biggest use cases for SIEM
- It's Subjective
- IDS largely responsible

The Numbers

Unique number of log types

IDS Rules	UTM Device	Firewall	Windows	Database
65939	11042	766	563	183

What Would You Do?

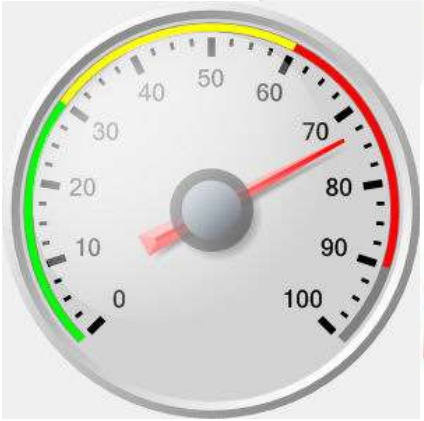
So which is more important?

- Jul 7 10:55:56 srbarriga sshd(pam_unix)[16660]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=192.168.20.111 user=root
- 2007-03-03 10:23:40 24.252.248.163 - W3SVC3 SERVER55 192.168.1.15 80 GET /images/9a.jpg - 200 0 32022 324 47 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+1.1.4322) - http://www.yahoo.com/
- Sep 7 06:25:28 PIXName %PIX-6-302013: Built inbound TCP connection 141968 for db:10.0.0.1/60749 (10.0.0.1/60749) to NP Identity Ifc: 10.0.0.2/22 (10.0.0.2/22)
- 200.96.104.241 - - [12/Sep/2006:09:44:28 -0300] "GET /modules.php?name=Downloads&d_op=modifydownloadrequest&%20lid=-1%20UNION%20SELECT%200,username,user_id,user_password,name,%20user_email,user_level,0,0%20FROM%20nuke_users HTTP/1.1" 200 9918 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)”
- Sep 1 10:38:36 10.10.10.1 614: *Sep 1 17:36:34.303: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:59633 -> 10.10.10.10:80]

Is There Any Easier Way?

Math!

- Assign a numerical priority to an Event
- Make comparison
- 5 > 2
  - Easy Button
- Risk Algorithms



CORRELATION

Correlation

Don’t confuse me with your words

Correlation – The process of creating new information from one or more possibly disparate information sources.

Correlation: Aggregation

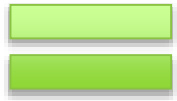
Not actually Correlation but…

- Happens after Normalization
- Generally occurs in the Correlation Engine
- Some SIEMS do their “counting” during Aggregation
- Aggregation can lose information

Correlation: Aggregation

Not actually Correlation but…

```
May 21 20:22:28 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
May 21 20:22:29 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
May 21 20:22:30 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
May 21 20:22:31 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
May 21 20:22:32 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
```



```
May 21 20:22:33 Multiple Failed Logins from 192.168.20.185 for user root
```

Correlation: Thresholds

An extension of Aggregation

- Something happens N times
- Something happens in X timeframe
- Something is of X priority or higher
- Thresholds can be applied to any Normalized data field

Correlation: Thresholds

An Extension of Aggregation

```
May 3 05:15:42.790 UTC: %SEC-6-IP: list 199 permitted tcp 10.131.5.17(3737) -> 10.0.4.101(22), 1 packet
May 3 05:15:44.404 UTC: %SEC-6-IP: list 199 denied tcp 10.131.5.17(3738) -> 10.0.4.101(445), 1 packet
May 3 05:15:44.790 UTC: %SEC-6-IP: list 199 permitted tcp 10.131.5.17(3739) -> 10.0.4.101(80), 1 packet
May 3 05:15:45.404 UTC: %SEC-6-IP: list 199 denied tcp 10.131.5.17(3740) -> 10.0.4.101(135), 1 packet
May 3 05:15:46.790 UTC: %SEC-6-IP: list 199 permitted tcp 10.131.5.17(3741) -> 10.0.4.101(143), 1 packet
May 3 05:15:47.404 UTC: %SEC-6-IP: list 199 denied tcp 10.131.5.17(3742) -> 10.0.4.101(123), 1 packet
May 3 05:15:48.790 UTC: %SEC-6-IP: list 199 permitted tcp 10.131.5.17(3743) -> 10.0.4.101(79), 1 packet
May 3 05:15:49.404 UTC: %SEC-6-IP: list 199 denied tcp 10.131.5.17(3744) -> 10.0.4.101(443), 1 packet
```

Rule: `If Unique(dest_port) > 5 then`

Alert: `Portscan detected from host 10.131.5.17`

Correlation: Logical

(Not(P)) if and only if (not(Q))

- IF [this] && [that]
  - THEN [dothis]
- IF “User_Login” && TimeOfDay > 20:00
  - THEN ‘Possible Account Compromise’
- IF count(SRC_IP) > 100 && event(‘SYN’)
  - THEN ‘DDOS’

WAIT THERE'S MORE!

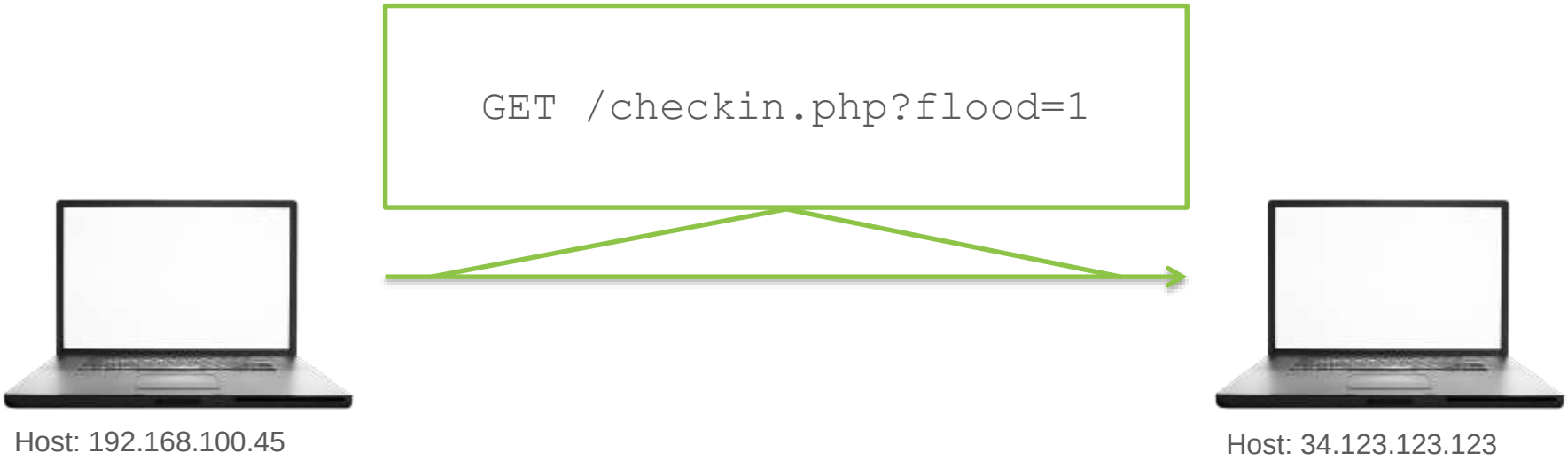
Context Enrichment

It’s not what I said, it’s where I said it…

- Adding Context to events helps you examine risk
- Context Enhancement is still “new” to SIEM

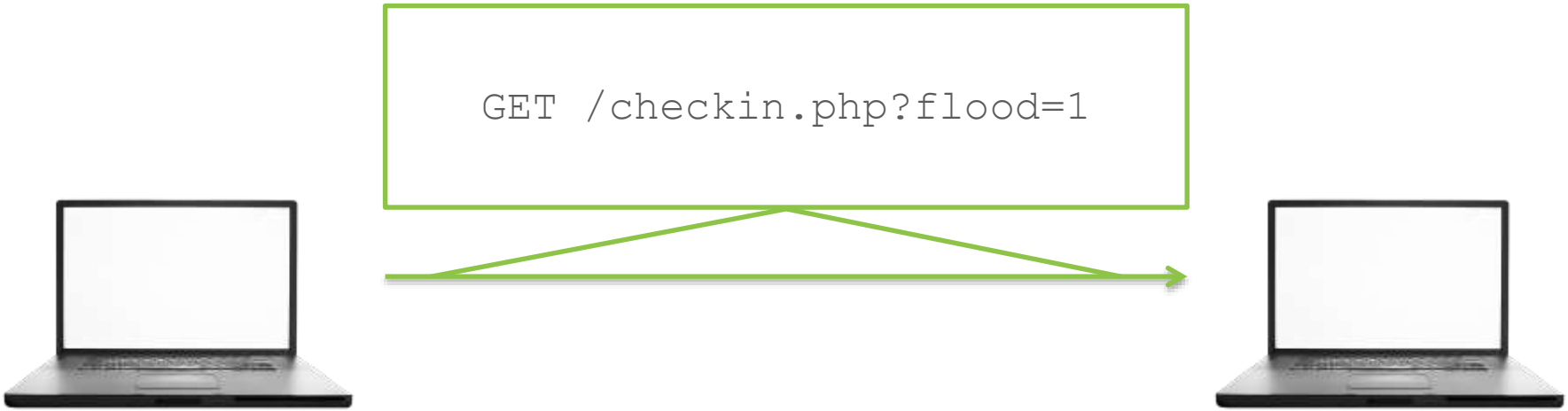
Context

Before



Context

After



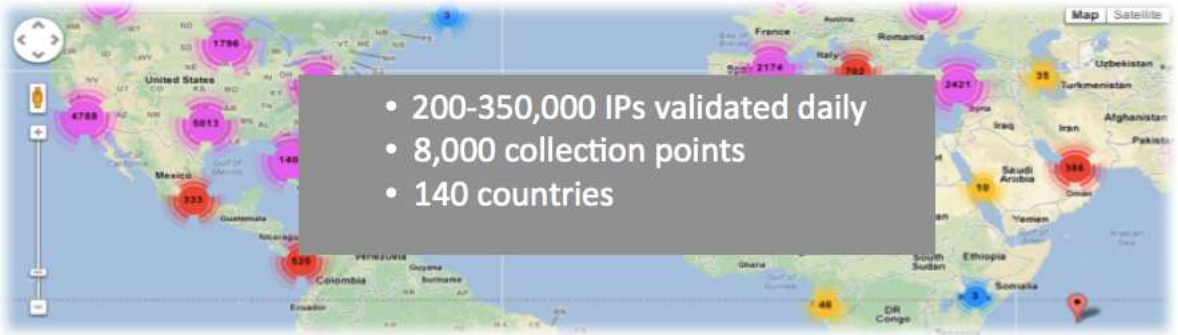
Host: 192.168.100.45
Hostname: prodweb01
Role: Server
Ports: 22, 80, 1337
OS: Windows XP (Really?)

Host: 34.123.123.123
Threat Intel: Known C&C
No Events in last Month
Web Server: [Unknown]
Location: EvilAxisCountry

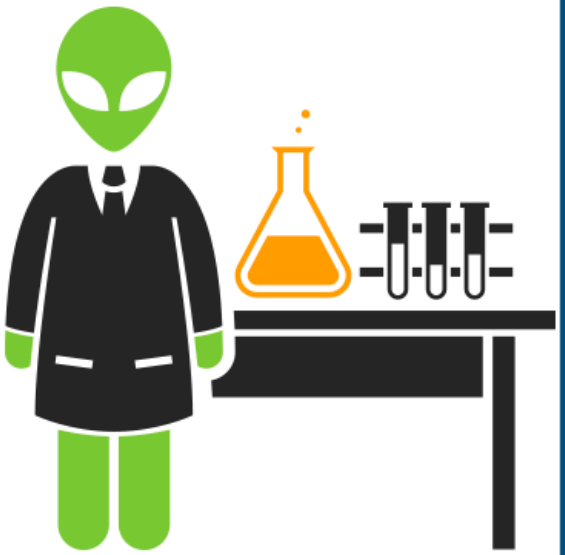
Threat Intelligence

AlienVault Open Threat Exchange™ (OTX)

Coordinated Analysis, Actionable Guidance



Join OTX: www.alienvault.com/open-threat-exchange



@AlienVault

Why Use SIEM?

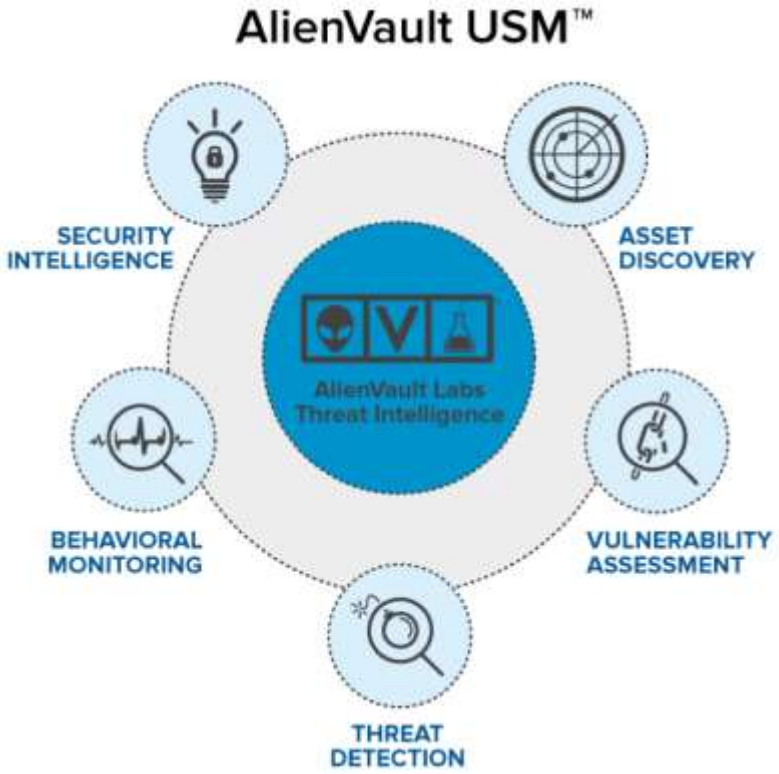
- Security – duh
- Compliance
- Monitoring
- Operations

EPS !$%@#$

Events Per Second

- Like the Cake, it’s a lie [most of the time]
- Real-Time
- Batch Processing (collection)

AlienVault Unified Security Management



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

Vulnerability Assessment
- Network Vulnerability Testing
- Remediation Verification

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

Behavioral Monitoring
- Log Collection
- Netflow Analysis
- Service Availability Monitoring

Security Intelligence
- SIEM Event Correlation
- Incident Response

Now for some Q&A

Test Drive AlienVault USM

- Download a Free 30-Day Trial

  http://www.alienvault.com/free-trial

- Try our Product Sandbox

  http://www.alienvault.com/live-demo-site

Questions? Email: hello@alienvault.com

Contact us on Twitter:

- Joe Schreiber @pkt_inspector
- Garrett Gross @garretthgross

@AlienVault