YOU BUILD SIEM
I DON'T ALWAYS LOOK AT DASHBOARDS

BUT WHEN I DO, I NEED PRETTY PICTURES
Internet had lots of examples and tutorials for specific or advanced dashboards

Top 10 lists of other things were easy to find

But no dashboard Top 10 list

Which led to.....
Quick Win, Industry Agnostic, SIEM Dashboards

Craig Bowser
Introduction

15+ years in InfoSec

Worked mainly in DoD with some DOJ and now DOE experience

GSEC GCED CISSP, yeah!

Christian, Father, Husband, Geek, Scout Leader who also does some woodworking

To Do List > To Do Open Slots
Criteria for Dashboards

1. Must use data types that are easy to ingest
2. Must use data from types of devices typically first 'connected' to SIEM
3. Must be simple to create
4. Must be relevant in any SOC
5. Must be able to visually convey information in a way that directs further investigation
Dashboard

What does this dashboard tell you?

What are the important things you should know when you view this dashboard?

Impact:

Correlations
Impact
Challenge
Examples
Dashboard

What you can cross reference the data with to determine more about the events?

What other events can you use to make a better decision regarding events seen?
<table>
<thead>
<tr>
<th>Column A</th>
<th>Column B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>IP ≜ Hostname</td>
</tr>
<tr>
<td>Filename/Hash</td>
<td></td>
</tr>
</tbody>
</table>
Dashboard

What issues are there that make this dashboard hard to use?

What problems cause the important events in this dashboard to be missed?
What are examples, from real life if possible, of how this dashboard was used to resolve actual issues?

Examples:
Cyber Kill Chain ©

Reconnaissance - Determine who, what and how of attack

Delivery - Initiate the attack

Installation - Solidify presence, create recurrence

Action on Objectives - Spread laterally, search for additional targets, go after goals

Weaponization - Craft methodology and capability to attack using what you learned during recon phase

Exploitation - Execute the attack, establish a foothold

Command & Control - Establish communication links, ensure open channels
Traffic World Map

Correlations

Impact

Challenge

Examples
Impact:
Management Eye Candy. Alert when node is down

Traffic World Map

Impact:

Impact:

Impact:

Impact:

Challenge

Examples
Impact


Challenge

Examples

Traffic World Map
Traffic World Map

Challenge:
Getting GPS coordinates of sites properly into SIEM
Traffic World Map

Examples:
DDOS attacks,
Detect new devices/connections

Impact
Challenge
Examples
# Alerts for New Devices/Software

<table>
<thead>
<tr>
<th>IP</th>
<th># Times Seen</th>
<th>Date First Seen</th>
<th>Date Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>3</td>
<td>26 July 2015</td>
<td>27 July 2015</td>
</tr>
<tr>
<td>1.0.0.2</td>
<td>10</td>
<td>20 July 2015</td>
<td>9 Aug 2015</td>
</tr>
<tr>
<td>1.0.0.3</td>
<td>1</td>
<td>1 Aug 2015</td>
<td>1 Aug 2015</td>
</tr>
<tr>
<td>1.0.0.4</td>
<td>35</td>
<td>5 Aug 2015</td>
<td>11 Aug 2015</td>
</tr>
</tbody>
</table>
Impact:
Discover and investigate unapproved software and devices

Alerts for New Devices/Software

Impact:
Installation

Impact:
Exploitation

Impact:
Challenge

Impact:
Examples
Correlations: Suspicious connections, large data transfers, CM approvals
Alerts for New Devices/Software
Alerts for New Devices/Software

**Challenge:**
Controlling large and decentralized networks. Keeping approved list updated.

**Impact**

**Correlations**

**Installation**

**Exploitation**

**Examples**
Alerts for New Devices/Software

Examples:
- Discovered contractor PCs, unauthorized web servers

Impact

Exploitation

Installation

Challenge

Examples
Impact

Correlations

Challenge

Examples

Vulnerability Statistics

Microsoft Windows Journal Remote Code Execution Vulnerability (MS15-045)
Microsoft Windows Shell Remote Code Execution Vulnerabilities (MS15-020)
Adobe Flash Player Multiple Remote Code Execution Vulnerabilities (APSB15-06)
EOL/Obsolete Software: Oracle Java SE/JRE/JDK 6/1.6 Detected
Microsoft Graphics Component Remote Code Execution Vulnerability (MS15-035)
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034)
Microsoft Internet Explorer Cumulative Security Update (MS15-032)
EOL/Obsolete Software SNMP Version Detected
EOL/Obsolete Software: Microsoft XML Parser and Microsoft XML Core Services (MSXML) 4.0 Detected
Oracle Java SE Critical Patch Update - January 2015
Vulnerability Statistics

**Impact:**
See the areas of most risk by class of vulnerability

**Challenge:**

**Examples:**
Correlations: IDS and AV to see what machines are most vulnerable to attack
Challenge: Eliminating false positives, determining vulnerability mitigations

Impact

Examples
Examples:
Using trends, determined effectiveness of patching tool.

Vulnerability Statistics
Top AV/HIPS Alerts

Today - 1 week
- Port Scan Detected: 10
- Conficker: 9
- MyDoom: 8
- PoisonIvy: 7
- I Love You: 6

Challenge
Examples
Top AV/HIPS Alerts

Impact:
ID Compromises, Outbreaks

Exploitation

Challenge
Examples
Correlations: 
Netflow, proxy, IDS and email logs to determine infection vectors

Top AV/HIPS Alerts

Impact

Correlations

Challenge

Examples

Exploitation
Challenge:
False positives, updating signatures, ineffectiveness of AV

Impact
Correlations
Examples

Exploitation
Examples: Detect unauthorized tools, unauthorized users ‘researching’

Top AV/HIPS Alerts

Impact

Correlations

Challenge

Examples

Exploitation
Top Firewall Denies Ext → Int

- 9.8.7.6
- 127.0.0.1
- 54.76.233.2
- 172.45.7.23
- 43.75.9.4
- 8.8.8.8
- 53.74.53.4
- 65.4.32.31.64
- 23.6.87.43
- 34.236.78.65

Correlations
Impact
Challenge
Examples
Top Firewall Denies Ext → Int

Impact:
ID top scanners, Recognize changes in automated attacks, Brute force attacks
Top Firewall Denies Ext → Int

Correlations:
IDS, Newly announced app vulns, Threat Intel

Impact
Challenge
Examples

Reconnaissance
Challenge: Sorting through noise, Verifying legit exceptions

Top Firewall Denies Ext → Int

Reconnaissance

Impact

Examples
Examples:
Detect port scans, port knockers, C&C bot controllers

Impact

Challenge

Examples:
Top Firewall Denies Int → Ext

Impact:
Detect policy evaders,
Suspicious traffic

Challenge
Examples

C2
AOO
Correlations: AV, IDS, DLP, CM approvals

Impact

Challenge

Examples

Top Firewall Denies Int → Ext
Top Firewall Denies Int → Ext

Challenge: Verifying legit exceptions, ID'ing crazy stuff

Impact

Examples

C2 AOO
Examples: Vendors who don’t allow their “call home” to be disabled
Top IDS Alerts  Ext → Int

- OS-WINDOWS Microsoft Groove mso.dll dll-load exploit...
- Transporter Beam detected
- INDICATOR-COMPROMISE Suspicious .cn dns query...
- SQLi attempt
- PROTOCOL-DNS dns cache poisoning attempt
- SMTP_RESPONSE_OVERFLOW (124:3) high Attempted User...
- FILE-PDF Microsoft Windows kernel-mode drivers core font...
- Patty-Cake-Patty-Cake
- http_inspect: HTTP RESPONSE HAS UTF CHARSET WHICH...
- Port Scan Detected

Correlations
Impact
Challenge
Examples
Top IDS Alerts  Ext → Int

**Impact:**
See suspicious traffic entering network, determine efficiency of F/W

---

Reconnaissance
Correlations:
AV, Firewall, Threat Intel, Vulnerability Scan Results

Top IDS Alerts Ext → Int

Reconnaissance

Impact
Challenge
Examples
Challenge: Tuning IDS, filtering false positives

Reconnaissance
Top IDS Alerts  Ext → Int

Examples:
Discovered vuln vendor had not stopped scan after contract ended

Reconnaissance

Impact

Challenge

Examples:
Impact:
See suspicious traffic leaving network

Top IDS Alerts Int  →  Ext

Impact
Correlations
Challenge
Examples

See suspicious traffic leaving network

C2  AOO
Top IDS Alerts Int → Ext

Correlations:
AV, DLP, Sensitive Data

Impact

Challenge

Examples
Top IDS Alerts Int → Ext

Challenge:
Tuning IDS, filtering false positives

Impact

Examples
Examples:
Unauthorized protocols (ie IRC, P2P), Infected systems

Impact
Challenge
Examples
Logon Successes

- Mouse
- Apoc
- Tank
- Cypher
- Switch
- Trinity
- Morpheus
- Neo

0 2000 4000 6000 8000 10000 12000

Correlations
Impact
Challenge
Examples
Logon Successes

Impact:
ID hard coded passwords, misused accounts

Correlations
Challenge
Examples

Installation
Correlations:
Logon failures, New accounts created, New devices/ apps
Impact
Installation
Correlations
Challenge
Examples

Challenge:
IDing service account ownership, how to handle machine accounts
Logon Successes

Examples:
- ID'd misused admin accounts and those coded in scripts
Logon Failures

**Impact:**
Identify suspicious account activity, misconfigurations

**Delivery**

**Challenge**

**Examples**
Logon Failures

Correlations:
- Account/Device type
- Timeline/locations of failures

Delivery
Impact
Challenge
Examples
Logon Failures

**Challenge:**
Clearing out false positives, getting OPS to fix 'unimportant' accounts

**Impact**

**Examples**

**Delivery**
Logon Failures

Examples:
Batch script with username/password unauthorized machines
Dashboards left off list

IDS Alerts Int → Int

Netflow by Total MB

Unique or Rare Ports used

Unique or Rare IDS hits

Firewall accepts Ext → Int
  Perform passive asset detection
Summary

Dashboards designed for quick setup, ease of use, but may be replaced long term.

Must use these dashboards in correlation with other information to obtain actionable data

Will discover many configuration and operational issues at first
  - need to clear out or ignore this noise to see important events

Able to provide simple initial overview of security posture of Enterprise
Next Steps

Tie FISMA into each dashboard?

20 Critical Controls

Solicit more input, discussions

FEEDBACK Welcome

reswob10@gmail.com is best

@reswob10 for twitter
When somebody writes, "call if you have any questions," Do they really mean ANY questions? Because I'm really wondering about platypuses.
BACKUP SLIDES
Impact: See suspicious lateral movement inside network, Insider Threat

Challenges:

Examples:

Top IDS Alerts  Int → Int
Top IDS Alerts Int → Int

Correlations:
Logon successes/failure, machines types traffic types

Impact
Challenges
Examples
Installation
Challenge: Investigating misconfigurations & allowed protocols/ports

Top IDS Alerts Int → Int

Impact

Installation

Examples
Top IDS Alerts Int → Int

Examples:
Unauthorized protocols and connections, P2P, suspicious lateral movement

Impact
Challenge
Examples
Installation
Impact: See suspicious connections
Correlate with: firewall, IDS, netflow activity to determine full extent of activity
Challenge: Keeping blacklist current (remove outdated entries, update new ones)
Examples: Discovering hijacked web sites with redirects
CKC – C2
Activity against inactive accounts  
BONUS # 2

Impact: See suspicious user activity
Correlate with: authentication failures, access to sensitive network locations, suspicious traffic
Challenge: Keeping list current, coordinating with HD when accounts are reactivated
Example: Found several accounts that were used to configure a service that runs rarely.
CKC – Exploitation