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 types of data that is easy to ingest
2. Must use data from types of devices typically '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:
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></td>
<td>Username</td>
</tr>
<tr>
<td></td>
<td>IP ↔ Hostname</td>
</tr>
<tr>
<td></td>
<td>Filename/Hash</td>
</tr>
</tbody>
</table>
Dashboard

Challenge:

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

What problems cause the important events in this dashboard to be missed?

Correlations  Impact
Challenge  Examples
Dashboard

What are examples, from real life if possible, of how this dashboard was used to resolve actual issues?

Examples:
Cyber Kill Chain ©

1. Reconnaissance
   - Determine who, what and how of attack

2. Delivery
   - Initiate the attack

3. Installation
   - Solidify presence, create recurrence

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

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

6. Exploitation
   - Execute the attack, establish a foothold

7. Command & Control
   - Establish communication links, ensure open channels
Information About Your Enterprise

Information of what is moving Around Your Enterprise

Information of what/who is On Your Enterprise
Impact: Management Eye Candy. Alert when node is down
Traffic World Map

Correlations:
- Nagios/OpenView
- Traffic Spikes
- High bandwidth usage

Impact
Challenge
Examples
Challenge: Getting GPS coordinates of sites properly into SIEM

Traffic World Map
Alerts for New Devices/Software

Sir, there are six of them, bearing 2, 1, 5, range 150 mi. ACHOOO!!!

And a blimp! A big shiny blimp slowly moving south!
Alerts for New Devices/Software

Impact:
Discover and investigate unapproved software and devices

Exploitation → Installation → Challenge → Examples
Alerts for New Devices/Software

**Correlations:**
- Suspicious connections, large data transfers, CM approvals

---

**Impact**

**Challenge**

**Examples**
Alerts for New Devices/Software

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

Impact

Examples

Installation

Exploitation
Alerts for New Devices/Software

Examples:
- Discovered contractor PCs, unauthorized web servers

Impact

Exploitation

Installation

Examples:

Discovered contractor PCs, unauthorized web servers
Vulnerability Statistics

Impact

Correlations

Challenge

Examples
Impact:
See the areas of most risk by class of vulnerability
Vulnerability Statistics

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

Examples:
Using trends, determined effectiveness of patching tool
Top AV/HIPS Alerts
Top AV/HIPS Alerts

Impact:
ID Compromises, Outbreaks

Exploitation

Challenge
Examples
Top AV/HIPS Alerts

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

Exploitation

Challenge

Examples

Impact

10 9 8 7 6 5 4 3 2 1
Top AV/HIPS Alerts

Challenge:
False positives, updating signatures, ineffectiveness of AV

Impact
Correlations
Examples
Exploitation
Top AV/HIPS Alerts

Examples:
Detect unauthorized tools, unauthorized users ‘researching’

Impact

Challenge

Exploitation
Top Firewall Denies Ext → Int
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

Reconnaissance

Impact
Challenge
Examples
Top Firewall Denies Ext → Int

Challenge:
Sorting through noise, Verifying legit exceptions

Reconnaissance
Top Firewall Denies Ext → Int

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

Reconnaissance
Top Firewall Denies Int $\rightarrow$ Ext

**Impact:**
Detect policy evaders, Suspicious traffic
Top Firewall Denies Int → Ext

Correlations:
AV, IDS, DLP, CM approvals
Challenge:
Verifying legit exceptions, ID'ing crazy stuff

Top Firewall Denies Int → Ext
Top Firewall Denies Int $\rightarrow$ Ext

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

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

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

Top IDS Alerts Ext → Int

Reconnaissance

Impact

Challenge

Examples
Top IDS Alerts  Ext $\rightarrow$ Int

**Challenge:** Tuning IDS, filtering false positives

- Impact
- Examples
- Reconnaissance
Top IDS Alerts  Ext → Int

Examples:
Discovered vuln vendor had not stopped scan after contract ended
Top IDS Alerts Int $\rightarrow$ Ext

Impact:
See suspicious traffic leaving network

Challenge
Examples

C2
AOO
Top IDS Alerts Int $\rightarrow$ 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 (i.e., IRC, P2P), Infected systems

Top IDS Alerts Int → Ext

Impact
Examples
Challenge
Examples
Logon Successes
Logon Successes

Impact:
ID hard coded passwords, misused accounts

Correlations

Installation

Challenge

Impact

Examples
Logon Successes

Correlations:
- Logon failures
- New accounts created
- New devices/apps
Challenge: IDing service account ownership, how to handle machine accounts

Logon Successes
Logon Successes

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

Correlations

Impact

Challenge

Examples
Logon Failures

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

**Delivery**

**Challenge**

**Examples**

---

10 9 8 7 6 5 4 3 2 1
Logon Failures

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

- Impact
- Challenge
- Examples

Delivery
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
Top IDS Alerts  Int $\rightarrow$ Int

Impact:
See suspicious lateral movement inside network, Insider Threat

Impact:
Installation

Challenge
Examples
Top IDS Alerts Int $\rightarrow$ Int

**Correlations:**
- Logon successes/failure,
- machines types
- traffic types

**Impact**

**Installation**

**Challenges**

**Examples**
Challenge: Investigating misconfigurations & allowed protocols/ports
Top IDS Alerts Int $\rightarrow$ Int

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

Impact

Examples:

Installation
URL hits against blacklist
BONUS # 1

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