

Re-writing the CSIRT Playbook



Jeff Bollinger – Infosec Investigator
Matt Valites - Infosec Investigator



19 Data Sources

Cisco Public © 2013 Cisco and/or its affiliates. All rights reserved.

splunk > 1TB Data Indexed / Day



NetFlow: 15.6 Billion flows / day

Cisco Public © 2013 Cisco and/or its affiliates. All rights reserved.

```
;; QUESTION SECTION:  
;first.org.
```

```
IN      A
```

2.5 Trillion DNS lookups / Day

The Splunk logo, featuring the word "splunk" in a white, lowercase, sans-serif font, followed by a white greater-than sign (>). The logo is set against a dark blue rectangular background.

Passive DNS

Lancope.

dce-cli - CLI for the Device Context Engine

The BMC Software logo, featuring a blue stylized icon of three triangles pointing left, followed by the text "bmcsoftware" in a blue, lowercase, sans-serif font.The GIR logo, featuring the letters "GIR" in a large, bold, white, sans-serif font with a slight glow effect.

Multiple Data Repositories

Cisco Public © 2013 Cisco and/or its affiliates. All rights reserved.

Our Mission

Mission:

- Protect Cisco by developing security monitoring architecture and strategy
- Respond to security threats using ad-hoc and **prescribed methods** of incident detection and response

How did we get here?

Effective CIRTs **must** evolve with changes in the cyber threat landscape to remain relevant.

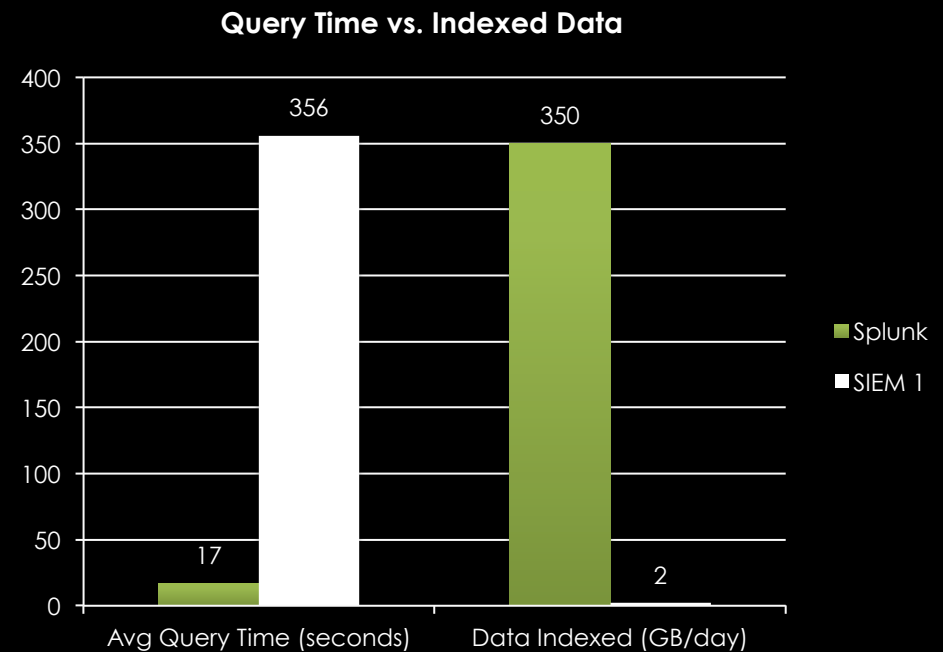
Over the last 11 years:

- Organic **evolution**
- Team **growth**
- Dramatic **increase in value and scope** of service offering

More information, more problems

My Data is Bigger

Index	Total Count (24 hours)
syslog	2,196,902,891
ad	1,054,349,972
wsa	426,229,009
acns	228,283,446
esa	49,836,291
dhcp	20,734,821
vpn	17,340,902
acs	15,785,442
ids	2,907,842
csa	682,527
edcs	549,044
sinkhole	282,399
dns	168,460
epo	42,775
fireeye	4,797
altiris	349



My Data is Bigger

The old way:

- Buy and trust a SIEM to run canned reports
- Wait for updates from the vendor

Scaling Problems

Searches and reports New

Showing 1-100 of 483 items 1 2 3 4 5 next »

Search name	RSS feed	Scheduled time	Results per page
1_rep002_s1_t23_hlth-mfe-clips		2013-03-24 07:00	100
1_rep003_s1_t23_tmd-device-event-count		2013-03-24 07:00	100
1_rep007_s1_t23_tmd-top-firing-sigs		2013-03-24 07:00	100
1_rep009_s1_t13_trgt-crdo-to-not-out		2013-03-24 21:00	100
1_rep009_s1_t13_trgt-crdo-to-out		2013-03-24 21:00	100
1_rep009_s1_t13_trgt-not-out-to-crdo		2013-03-24 21:00	100
1_rep009_s1_t13_trgt-out-to-crdo		2013-03-24 21:00	100
1_rep015_s2_t03_mal-infect-bundle		2013-03-24 11:00	100
1_rep016_s2_t03_mal-64005-dmz		2013-03-24 11:00	100
1_rep017_s2_t03_mal-60001-60111		2013-03-24 11:00	100
1_rep021_s1_t03_mal-60007-temple-query		2013-03-24 11:00	100
1_rep021_s1_t04_mal-60007		2013-03-24 12:00	100
1_rep021_s1_t09_monthly-60007		2013-04-01 17:00	100
1_rep024_s1_t03_mal-irc-to-external		2013-03-24 11:00	100
1_rep024_s1_t03_mal-irc-to-internal		2013-03-24 11:00	100
1_rep027_s1_t02_inv-mfe-64003		2013-03-24 10:00	100
1_rep029_s1_t03_mal-64000		2013-03-24 11:00	100
1_rep034_s1_t00_inv-mfe-out-to-in		2013-03-24 08:00	100
1_rep034_s1_t01_inv-mfe-dc-to-dmz-dns		2013-03-24 09:00	100
1_rep034_s1_t01_inv-mfe-dc-to-out		2013-03-24 09:00	100
1_rep034_s1_t01_inv-mfe-in-to-dc		2013-03-24 09:00	100
1_rep034_s1_t01_inv-mfe-in-to-out		2013-03-24 09:00	100
1_rep034_s1_t02_inv-mfe-dc-to-in		2013-03-24 10:00:00 UTC	100
1_rep034_s1_t02_inv-mfe-dmz-dns-to-dc		2013-03-24 10:00:00 UTC	100
1_rep034_s1_t02_inv-mfe-dmz-dns-to-dmz-dns		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t01_inv-mfe-in-to-dmz-dns		2013-03-24 09:00:00 UTC	100
1_rep034_s2_t01_inv-mfe-out-to-dc		2013-03-24 09:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-dc-to-dc		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-dmz-dns-to-in		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-dmz-dns-to-out		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-in-to-in		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-in-to-out		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-out-to-out		2013-03-24 10:00:00 UTC	100
1_rep034_s2_t02_inv-mfe-out-to-in		2013-03-24 10:00:00 UTC	100

- SEIM unable to process reports during an analyst's shift
- Reports broken into multiple smaller 'directional based reports'
- Inefficient way to process data
- Led to inefficiency

9-13-11	Aug 27, 2012 3:40 PM	--	Folder
.DS_Store	Today 10:37 AM	6 KB	Document
all_sources.txt	Sep 13, 2011 10:59 AM	1 KB	Plain Text File
check event	Sep 13, 2011 11:54 AM	--	Folder
daily_sources.csv	Sep 13, 2011 3:21 PM	6 KB	comm...values
daily_sources.txt	Sep 13, 2011 11:19 AM	284 bytes	Plain Text File
daily_sources.xlsx	Sep 13, 2011 4:17 PM	57 KB	Micro...rkbook
Daily-virus-track-active.xls	Sep 13, 2011 2:49 PM	216 KB	Micro...rkbook
dhcp.txt	Sep 13, 2011 4:13 PM	54 bytes	Plain Text File
Infection_Tracking.xls	Sep 13, 2011 3:07 PM	143 KB	Micro...rkbook
IPs...xls	Dec 7, 2010 10:42 AM	15 KB	Micro...rkbook
irc	Sep 13, 2011 11:49 AM	--	Folder
.DS_Store	Sep 13, 2011 11:48 AM	6 KB	Document
1_rep024_s2_t03_mal-irc-to-external-CheckEvent-1315909826069.csv	Sep 13, 2011 11:23 AM	930 KB	comm...values
1_rep024_s2_t03_mal-irc-to-external-EventSummary-1315909826069.csv	Sep 13, 2011 6:30 AM	33 KB	comm...values
hl_results.csv	Sep 13, 2011 11:29 AM	12 KB	comm...values
hl.txt	Sep 13, 2011 11:25 AM	722 bytes	Plain Text File
irc.zip	Sep 13, 2011 11:48 AM	300 KB	ZIP archive
message_decoded.txt	Sep 13, 2011 11:28 AM	589 KB	Plain Text File
message_decoded.xlsx	Sep 13, 2011 11:36 AM	75 KB	Micro...rkbook
message.txt	Sep 13, 2011 11:26 AM	623 KB	Plain Text File
Malware	Sep 13, 2011 10:06 AM	--	Folder
.DS_Store	Sep 13, 2011 10:06 AM	6 KB	Document
Malware.zip	Sep 13, 2011 10:04 AM	8.3 MB	ZIP archive
nachi.txt	Sep 13, 2011 10:18 AM	2 KB	Plain Text File
notes.txt	Sep 13, 2011 4:19 PM	2 KB	Plain Text File
rep054.txt	Sep 13, 2011 10:19 AM	4 KB	Plain Text File
summaries	Sep 13, 2011 11:54 AM	--	Folder
.DS_Store	Sep 13, 2011 11:53 AM	6 KB	Document
1_rep015_s2_t03_mal-infect-bundle-EventSummary-1315908367680.csv	Sep 13, 2011 6:06 AM	7 KB	comm...values
1_rep016_s2_t03_mal-64005-dmz-EventSummary-1315908737428.csv	Sep 13, 2011 6:12 AM	20 KB	comm...values
1_rep017_s2_t03_mal-60001-60111-EventSummary-1315908565190.csv	Sep 13, 2011 6:09 AM	7 KB	comm...values
1_rep021_s2_t03_mal-60007-tem...ventSummary-1315909264283.csv	Sep 13, 2011 6:21 AM	3 KB	comm...values
1_rep024_s2_t03_mal-irc-to-external-EventSummary-1315909826069.csv	Sep 13, 2011 6:30 AM	33 KB	comm...values
1_rep029_s2_t03_mal-64000-EventSummary-1315909553321.csv	Sep 13, 2011 6:25 AM	6 KB	comm...values
1_rep054_s2_t03_mal-medium-fid...ventSummary-1315908893391.csv	Sep 13, 2011 6:14 AM	34 KB	comm...values
csa_scan_summary.txt	Sep 13, 2011 11:22 AM	3 KB	Plain Text File
summaries.zip	Sep 13, 2011 11:54 AM	15 KB	ZIP archive
Total Files	Sep 13, 2011 8:58 AM	--	Folder
Total_...xls	Sep 13, 2011 4:47 AM	817 KB	Micro...rkbook
Virus_Total_May_FY011Q1.xls	Sep 13, 2011 4:20 AM	1.1 MB	Micro...rkbook
Virus_Total_May_FY011Q1.xls	Sep 13, 2011 4:21 AM	6 MB	Micro...rkbook
Total_Alliance_FY11Q1.xls	Sep 8, 2011 7:49 AM	1.3 MB	Micro...rkbook
vpn.txt	Sep 13, 2011 4:10 PM	218 bytes	Plain Text File
V...	Sep 5, 2011 9:24 PM	70 KB	Micro...rkbook
9-13-11.zip	Sep 13, 2011 4:25 PM	21.7 MB	ZIP archive

- Static and inflexible
- Performance
- Expensive
- Limited
- Compatibility
- Retention

My Data is Bigger

The new way:

- Build your own collection infrastructure
- Build your own reports
- Research your own intelligence
- Operationalize and optimize

Dependencies

- Requires good architecture and a plan
- Requires smart people
- Scale and efficacy
- Data management

Currently

Search

[indexids mtvs-pki-ms-1 OR rtp5-dc-spf3-ms-1 AND signature=6965f AND attacker_locality="PKI" AND NOT target_locality="PKI" AND NOT target_locality="PKI_HOM"] | stats values(attacker) as "Source",values(attacker_locality) as "Source Locality",values(target) as "Destination",values(target_locality) as "Destination Locality" by target_port | rename target_port as "Destination Port"

[View raw search results](#) [Download CSV](#) [Download JSON](#) [Save](#) [Create](#)

Show results

16 results in the last 24 hours (from 1:00:00 AM March 23 to 1:21:11 AM March 24, 2015)

[Reset](#) [Export](#) [Options](#) 50 per page ▾

Overlay:	Name	Source	Destination Port	Source Locality	Destination	Destination Locality
1	111	171.68.34.153 171.68.34.154 171.68.34.155 171.68.34.156 171.68.34.157 64.102.106.27 64.102.106.40 64.102.106.48 64.102.106.56 64.102.106.69		PKI	10.28.21.229 171.70.145.234 64.102.18.131 64.102.18.132 64.102.120.6 64.102.17.50	DC_NETWORK_FILTERS DC_SERVERS DC_RTP_DC_NETS DC_SJ
2	1159	171.68.34.158 171.68.34.159		PKI	72.163.43.56	DC_ALL_DC_NETS
3	1234	171.68.34.154 171.68.34.155 171.68.34.156 171.68.34.157 171.68.34.171		PKI	171.70.145.234	DC_SJ
4	120	171.68.34.157		PKI	173.36.129.232	DC_OTHER_DC_NETS
5	10724	171.68.34.153 171.68.34.154 171.68.34.155 64.102.106.40 64.102.106.60 64.102.106.81		PKI	171.68.38.36 171.68.38.36	DC_ALL_DC_NETS
6	139	171.68.34.157		PKI	72.163.46.163	DC_AD_SERVERS
7	1024	171.68.34.141 171.68.34.153 171.68.34.154 171.68.34.155 64.102.106.40 64.102.106.60 64.102.106.81		PKI	173.37.163.235 173.37.163.237 173.37.163.238	DC_OTHER_DC_NETS
8	2049	171.68.34.163 171.68.34.155 171.68.34.156		PKI	10.28.21.229 171.70.145.234 64.102.55.14	DC_NETWORK_FILTERS DC_SJ

- 16 results
- Analyzed in Splunk
- Formats data during search

The Playbook



Cisco Public © 2013 Cisco and/or its affiliates. All rights reserved.

What is a playbook?

playbook | 'plā,bŏk|

noun

A prescriptive collection of repeatable queries (reports) against security event data sources that lead to incident detection and response.

0100003-HF-IDS-MALWARE:BOT-C2

Objective:

Discover and report botnet infected hosts for remediation and enhance future detection.

Working:

```
index="ids" earliest=-10m tag=HF-IDS NOT (tag=IN_DNS OR tag=DC_MBOX | stats count  
by host | sort -count limit=50 | rename attacker AS C2 | csirtTable | makeAcaseHF  
| botSquash(C2)
```

Action:

Case generated into auto-remediation queue: **CSIRT-Analysts-HF**

Analysis: The generated report is high fidelity – if an IRC Join is detected, verify the NICK is computer generated. These events require the reimaged malware remediation process. If the bot matches the [Infostealer List](#), email client [password update instructions](#). If the client address matches the [VIP list](#), those hosts must be escalated to the [on-duty investigator](#).

Reference: wiki/[10012](#), bugzilla:[576](#), GIR: n/a

Where do I Begin?

- What am I trying to **protect**?
- What are the **threats**?
- How do I **detect** them?
- How do we **respond**?

IR Fundamentals

- Develop requirements on frequency, priority, and scope
- Ensure basic requirements:
 - Solid systems of record
 - Complete traffic inspection coverage
 - Proper communication channels
 - Ensure proper remediation controls
 - Enforceable policies
- If you can build a good query, you can find malware, infected systems, and dedicated attackers
- If you can't automate, investigate

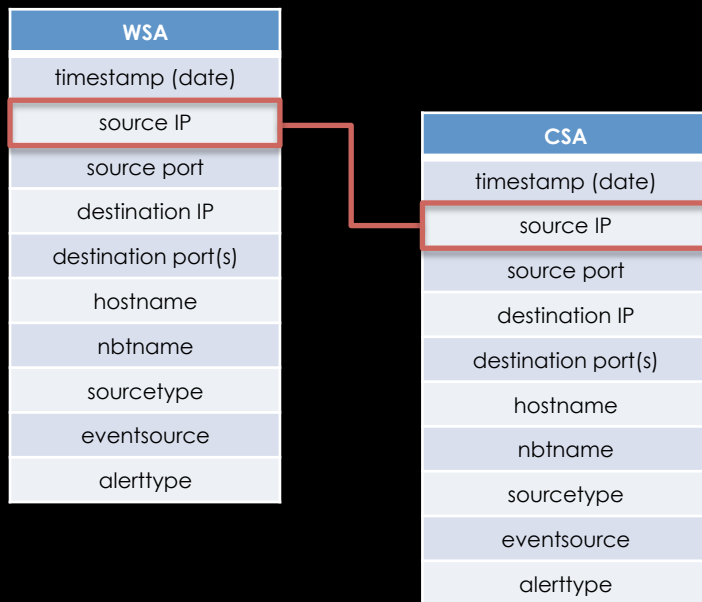
The Playbook MUST:

- Detect **malware** infected machines
- Detect **suspicious network activity**
- Detect **anomalous authentication attempts**
- Describe and understand **inbound AND outbound traffic**
- Provide **custom views** into certain environments

Additionally:

- Provide **summary information** including trends, statistics, counts
- Provide usable and quick access to **statistics and metrics**
- **Correlate** events across **all relevant data sources**

Correlation



Why?

- Attribution
- Confirmation
- Temporal correlation
- Concurrent multi-index search ("sub-search")

How?

- Union
- Join

0800001-INV-MULTI-MALWARE:WSA validation of attempted CSA network connections

Objective:

Searches HIDS for outgoing tcp/80 connections and uses those IPs to find corresponding WSA logs to determine if the HIDS detected connection was malicious or not.

Working:

```
index="wsa" x wbrs_threat_type="*" (NOT (cs_referer="*")) [search
index="csa" "attempted to initiate a connection as a client on TCP port 80" "allowed" |
  rex "on TCP port 80 to (?<csa_dst_ip>\d+\.\d+\.\d+\.\d+) using" |
  dedup csa_dst_ip |
  rename csa_dst_ip AS s_ip |
  fields s_ip] |
  rex field=cs_url "http:\\\\(?:<domain>[^\./]+)" |
  rex field=cs_url "\\(?:<script_name>[^\./?]+(?:=$|\\?)" |
  dedup script_name |
  dedup domain |
  dedup c_ip |
  dedup cs_url
```

Action:

Manual investigation. Analysis may result in submitting a host for remediation.

Analysis: Investigate whether HIDS detected connections may be a sign of an infected host by reviewing the WSA SIO data and any additional event indicators.

Reference: wiki/[10103](#), bugzilla:[6742](#), GIR: n/a

How do we know you're working?

METRICS!

- Top events fired per event source
- Top malicious domain
- Total infected hosts
- Top malware type/family
- Highest areas of infection (lab, DC, DMZ, etc.)
- Infections by theatre
- Infection by role/org (sales, engineering, marketing, etc.)
- Event rates and collection stats (total volume of alarms, then alarms by source, index/filesize avg/day)
- Unique user counts avg/day
- Total attacks blocked by CSIRT
- Top infections by event source (event source detection ranking)

Yeah, but how **exactly** do we do it?

Malware/Advanced Detection

e.g. Phishing URLs in email

Anomaly Detection

e.g. Two VPN logins from a single user

Policy-driven monitoring:

e.g. Flows from datacenter to Internet

Operational intelligence:

e.g. Malware analysis for indicator discovery

You can help!

- FIRST standard
- Information sharing – how do **YOU** detect threats?
- Strategy sessions (network agnostic)



Q/A

jeff.bollinger@cisco.com
matthew.valites@cisco.com