RAPID7

YOU'VE GOT 99 PROBLEMS AND A BUDGET'S ONE

Rebekah Brown | @PDXBek

Threat Intelligence Lead at Rapid7

But before that…

- Gunnery Sergeant United State Marine Corps
- Chinese Crypto linguist and Network Warfare Analyst
- Policy Developer
- Liaison to State and Local Governments
- Threat Intelligence in the private sector

Why are budgets such a problem?

We are living in a material world…

- Feeds - $$- $$$$
- Platform - $$$- $$$$
- Reports - $$-$$$$
- Analyst on Demand - $$$
- Social Media Analysis - $$- $$$$

2015 Global Study on IT Security Spending & Investment – Ponemon Institute

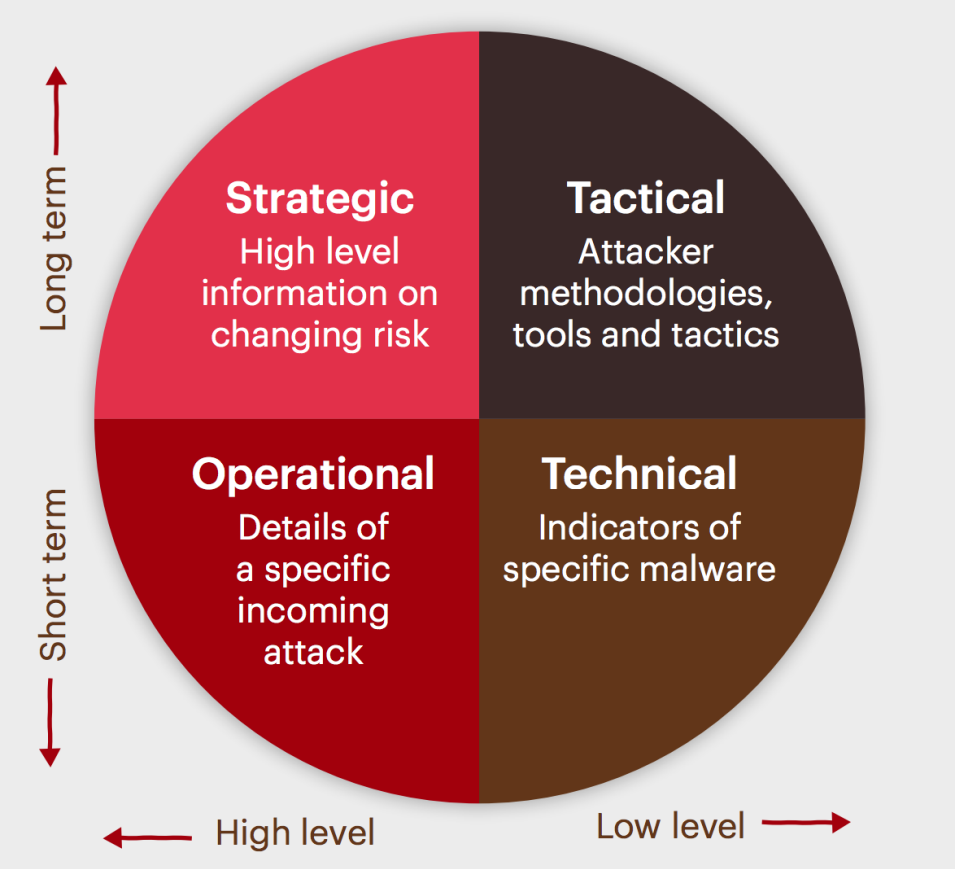
- 50% security budget is stalled or declining
- 19% IT security leadership has a say in resource allocation
- 37% of investments in security investments did not meet expectations
- Many organizations do not have the budget to even stay in compliance with regulations

Frugal Girl's Guide to Threat Intelligence

- Solid Foundation - FREE
- Open-source Feeds – FREE*
- Open-source Platforms – FREE*
- Open-source reports – FREE
- Community Tools – FREE*
- Smart friends - PRICELESS


Retreat, hell! We're not retreating, we're just advancing in a different direction.
— Oliver P. Smith —

That all sounds well and good… but how?



- CERT-UK and the Centre for the Protection of National Infrastructure
- https://www.cpni.gov.uk/advice/cyber/Threat-Intelligence/
- Strategic
- Operational
- Tactical
- Technical

Security Functions

- Risk and Priority Assessment
- Situational Awareness
- Threat Identification and Alerting

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	Assess threats facing similar businesses. Source: DBIR, industry reports, annual reports	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media	Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	Assess threats facing similar businesses. Source: DBIR, industry reports, annual reports	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media	Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	**Assess threats facing similar businesses.** **Source: DBIR, industry reports, annual reports**	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media	Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

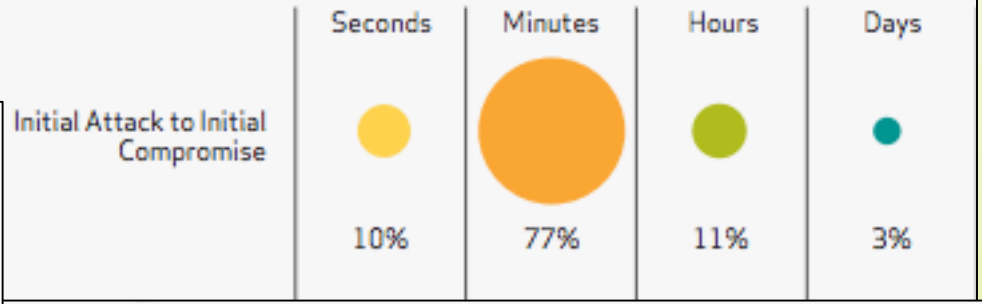
Strategic Intel for Risk and Priority Assessment

“What threats are facing us? What can we do to prevent it?”

- Goal: Assess threats facing business similar to yours and present that information in a digestible format
- Resources:
  - Verizon Data Breach Investigations Report
  - DBIR Industry Snapshot
  - Congressional Research Service
  - Internal resources

DBIR Industry Snapshot - Healthcare

Figure 4. Timespan of events by percent of breaches in the Healthcare industry



Close to two-thirds of all breaches go on for months before the victim learns that they've been compromised.

Table 1. Threat action varieties by percent of breaches in the Healthcare industry

Rank	Variety	Category	Breaches
1	Exploitation of default or guessable credentials	Hacking	72%
2	Backdoor (allows remote access/control)	Malware	49%
3	Exploitation of backdoor or command and control channel	Hacking	49%

CRS Reports for Congress

- Cybersecurity Policy
- Critical Infrastructure
- Cybercrime and Data Security
- Cybersecurity framework
- Reports by federal agency

Internal Resources

- Business Priorities
- Asset Management
- Third Party Outsourcing
- Security Posture

Key Points:

- What are the largest threats to organizations similar to yours?
- What types of threat actors target your organization?
- What actions do they take?
- Where do they attack?
- Are we positioned to identify and defeat an attack?

Tips for Reporting to the Board:

- Do not use jargon or overly technical terms
- Discuss business impact of threats
- Be prepared to answer questions
- Tell the story
- Keep it simple

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	Assess threats facing similar businesses. Source: DBIR, industry reports, annual reports	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	**Understand current or planned campaigns and how to respond** **Source: News, blogs, Industry reports, forums, social media**	Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	**Identify whether a current or planned attack is impacting you and determine how to respond.** **Source: Blogs, social media, forums.**	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

Operational Intel for Situational Awareness

“Is this attack that is happening going to impact us? Do we need to change anything to be prepared?”

- Goal: Understand ongoing or pending attacks and be prepared to respond.
- Resources:
  - Social Media
  - Blog Posts
  - Government Alerts
  - Partners and peers

Operational Intel for Situational Awareness

Threat Identification

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

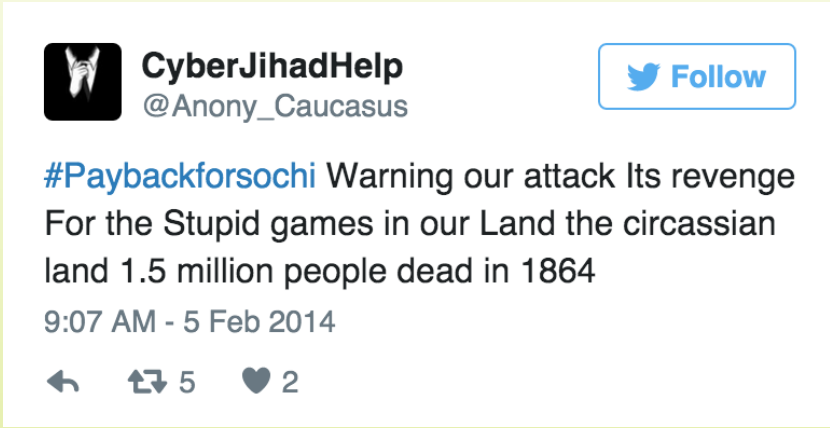
HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS

Security Tip (ST14-001)

Sochi 2014 Olympic Games

Original release date: February 04, 2014 | Last revised: March 10, 2014

Print | Tweet | Send | Share



CyberJihadHelp
@Anony_Caucasus

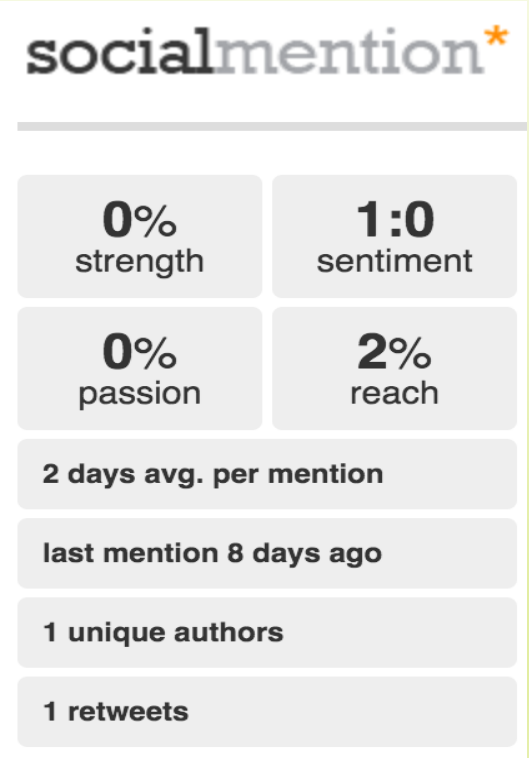
Follow

#Paybackforsochi Warning our attack Its revenge For the Stupid games in our Land the circassian land 1.5 million people dead in 1864

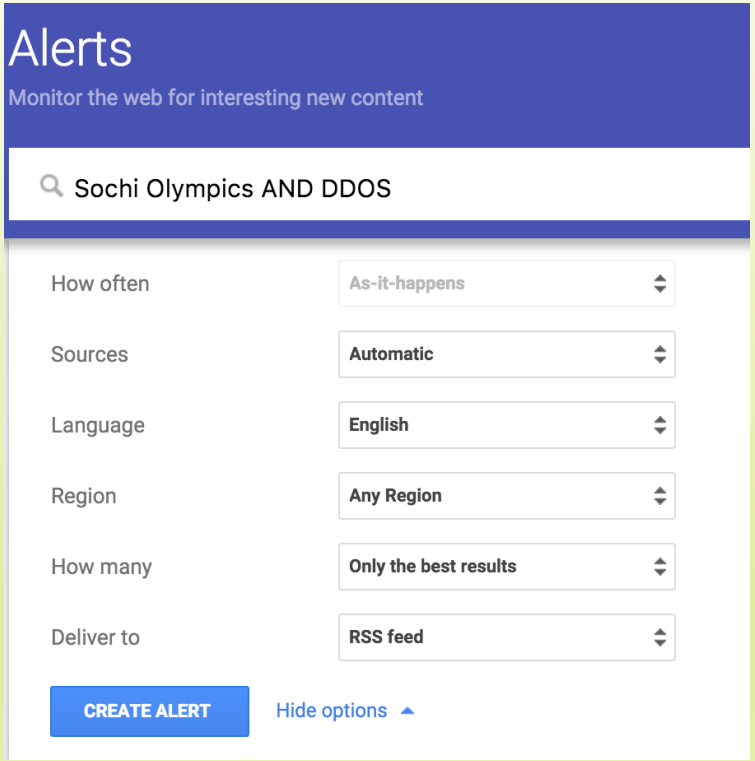
9:07 AM - 5 Feb 2014

5 2

Social Mention

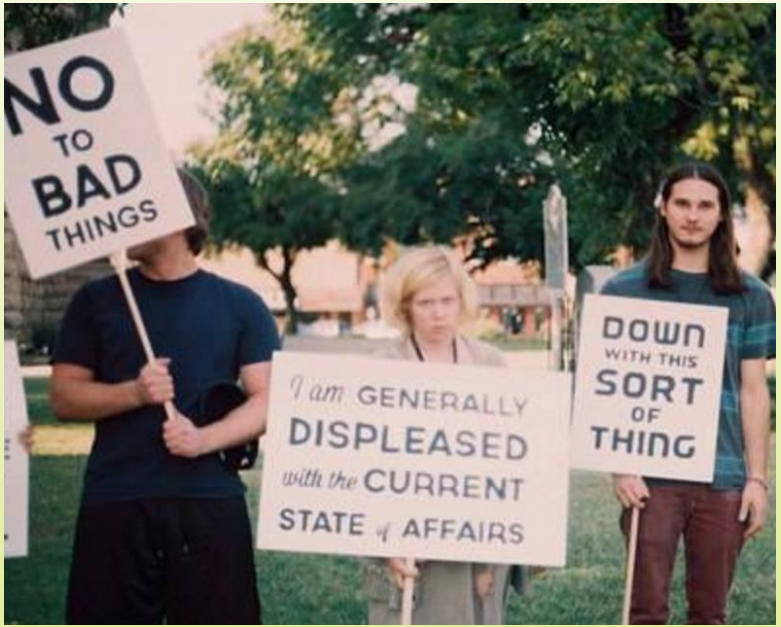


Google Alerts



Key Points:

- What is the operation?
- Who is the target?
- How have they attacked in the past?
- Are we vulnerable to any of those attacks?
- What are we seeing now that could help us defend ourselves?



Tips for Reporting

- Be objective
- Identify triggers
- Identify constraints – if this is serious what do you need to do your job?
- Provide updates

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	**Assess threats facing similar businesses.** **Source: DBIR, industry reports, annual reports**	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media	**Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports**	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	**Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.**	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

Tactical Intel for Situational Awareness

“Is this new tactic/tool/methodology going to impact us? How quickly do we need to respond?”

Goal: Identify TTPs or indications of a threat and determine how to alert and respond.

Resources:

- News
- Social Media
- Blog Posts
- Internal Resources

Tactical Intel for Situational Awareness

HD Moore's Law

"Casual Attacker power grows at the rate of Metasploit"

- Pay special attention to vulnerabilities with Metasploit modules
- More attacker activity
- Check your vulnerability
- Identify artifacts and IOCs to monitor

Metasploit Weekly Wrap Up

New Modules

This update also comes with a fun privilege escalation exploit for OSX where an environment variable ends up on a commandline. I love these kinds of bugs because people have been screwing up environment variables since the invention of shells.

As always, you can see all the changes since the last wrapup on github: 4.11.4-2015102801...4.11.5-2015103001

Exploit modules

- Th3 MMA mma.php Backdoor Arbitrary File Upload by Jay Turla
- Mac OS X 10.9.5 / 10.10.5 - rsh/libmalloc Privilege Escalation by rebel and shandelman116 exploits CVE-2015-5889

Auxiliary and post modules

- Joomla Real Estate Manager Component Error-Based SQL Injection by Nixawk and Omer Ramic
- Joomla com_contenthistory Error-Based SQL Injection by Asaf Orpani, Nixawk, and bperry exploits CVE-2015-7297

If you are vulnerable:

- Overview of the threat
- Details of how it operates
- What systems are at risk
- How those systems fit into operations
- Available remediation or workarounds

If you are NOT vulnerable:

- Not every threat will impact every organization!!!
- Provide an overview of the threat
- Details of how it operates
- WHY it should not impact you
- What to continue to look for

Tips for Reporting

- Technical terms are fine, but define if you have a broad audience
- Provide links to sources
- Use bullet points to call out important details
- TIMELINESS IS KEY
- Control the spin
- Update as needed

	Strategic Intelligence	Operational Intelligence	Tactical Intelligence	Technical Intelligence
Risk and Priority Assessment	Assess threats facing similar businesses. Source: DBIR, industry reports, annual reports	Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports	Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports	Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports
Situational Awareness	Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports	Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media	Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports	Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports
Threat Identification and Alerting	Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports	Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.	Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports	Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports
Hunting Operations	Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.	Information about attackers, where and how they communicate, who they target. Source: Social media,	Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs,	Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal

Technical Intelligence for Threat Alerting

“What is this thing??!?!”

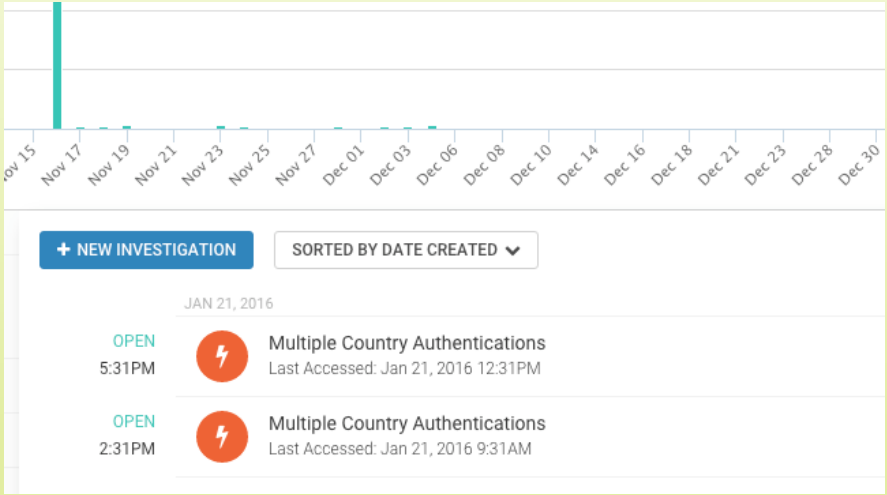
Goal: Make sense of alerts that the SOC has to deal with *because of you*

Resources:

- Virus Total
- Blogs
- Reports
- Maltego

What can you do?

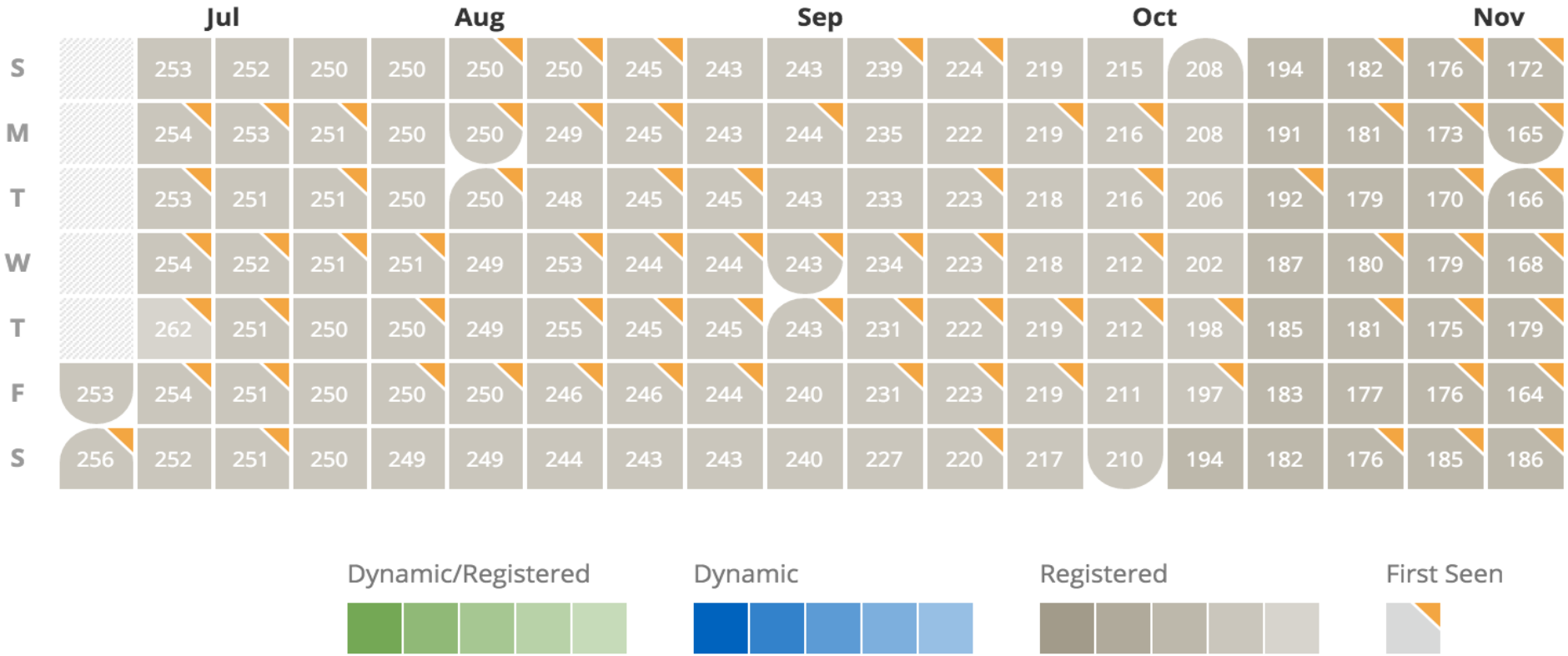
- You alerted on something for a reason – I hope
- Key Details:
  - Where did the alert come from?
  - When was it flagged as malicious?
  - What activity is it associated with?
- Identify false positives



Passive Total

72.167.232.198	US	72.167.232.0/24	2013-03-28 17:11:12	2015-01-20 03:55:09	riskiq, virustotal, kaspersky	godaddycom, apache, blocklist, bruteforcelogin
50.57.19.16	US	50.57.0.0/16	2012-03-21 21:13:23	2013-03-27 15:14:22	riskiq	rackspace_hosting
64.202.189.170	US	64.202.188.0/23	2011-02-12 17:02:20	2012-03-15 15:21:22	riskiq	hosting-provider, godaddycom

Heatmap | OSINT 2 | Potential Malware 56



72.167.232.198

ATTRIBUTES

First Seen	2009-09-01 05:24:22
Last Seen	2016-01-21 00:00:00
Resolutions	2096
Network	72.167.232.0/24
ASN	26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com)
Country	US
Ever Compromised?	true / false
Sinkhole	true / false

Heatmap | OSINT 2 | Potential Malware 56

Source	Link	Tags
Blocklist	http://www.blocklist.de/en/export.html	blocklist, apache
Blocklist	http://www.blocklist.de/en/export.html	blocklist, bruteforcelogin

Select a date or dates *(shift-click)* on the Heatmap to filter results.

Resolve	First	Last	Source
monumentalperformance.com	2016-01-21 00:00:00	2016-01-21 00:00:00	virustotal

72.167.232.198

ATTRIBUTES

First Seen	2009-09-01 05:24:22
Last Seen	2016-01-21 00:00:00
Resolutions	2096
Network	72.167.232.0/24
ASN	26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com)
Country	US
Ever Compromised?	true **false**
Sinkhole	true **false**

Heatmap | OSINT 2 | Potential Malware 56

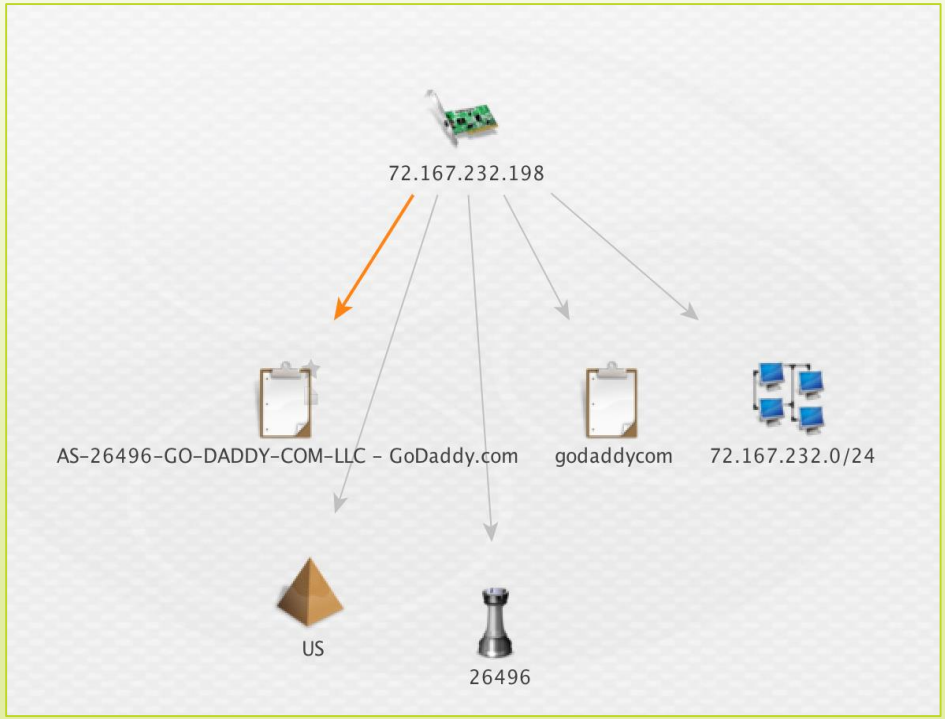
virustotal	6f617c4807b67fddcd8311b906ebb74349affe0325dababf4979146171fb0d6f
virustotal	704be96408ea78177f8b37005877b8cb6706c4d8d52d564a4d5dd9863903d470
virustotal	9d926f81a53f03e26684df997ef120afd75d96db50af45cd1b1f073792e05b8f
virustotal	1b7853eb397dd27684e21106087deab377eea50718ebdc23c5ae0158beef3234
virustotal	7399f0d45ac26b64b525d17a1414e06e48cec104a6040cb13cf224436ab0b106
virustotal	6c6c8e2aba8e8caa1011280c48c1daf12af30b44d8af28ec0b0e9e853626253b
virustotal	c4eaa520fa8422f76e12b41a078659ddce3e099945d6195fc8966b27e8dfec27
virustotal	7bae7cfa3d4ae981648faf0a4bc51b49cc7ab8d5f5f06cb6821e7a22049ce9cd
virustotal	c7592ff50a257760f6d00631dab439006589275e11f870be8aad880ab19509c8

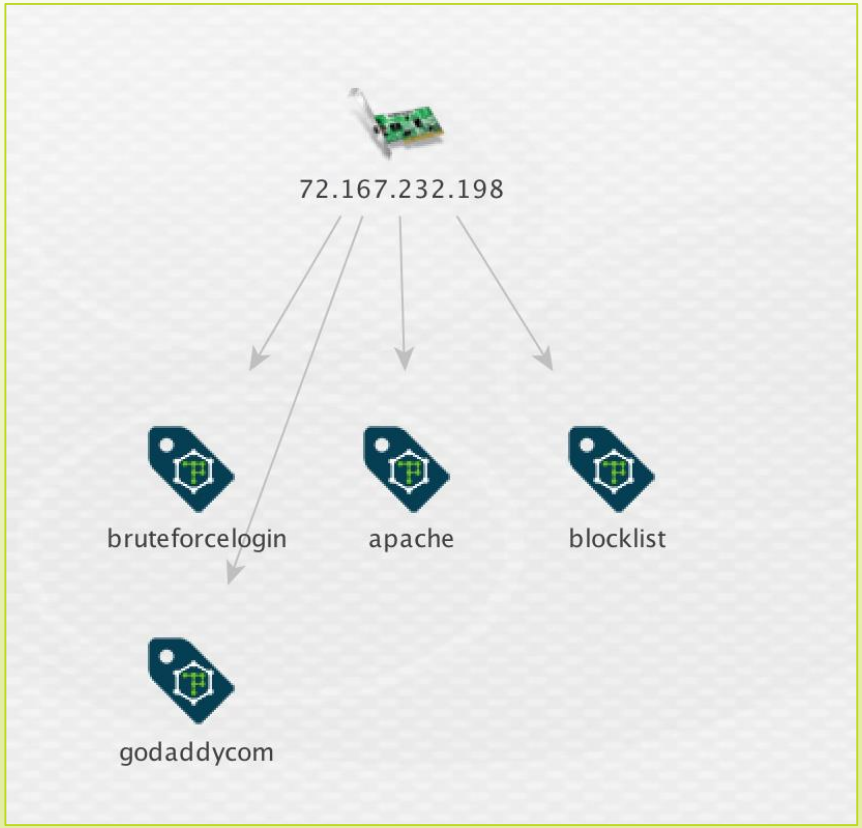
Maltego

- Passive Total
- Threat Crowd
- Paterva
- Build your own machines
- Developer Portal:

  http://dev.paterva.com/developer/

Passive Total Transforms





Tips for Reporting

- Develop a process
- Keep track of your findings
- Provide related indicators or behaviors
- Identify repeat offenders
- Refine your block or alert lists

Reporting on ROI (or lack thereof)

- Make summaries
- Capture the impact
- What worked?
- What didn’t?
- What needs to be changed?
- Where are the pain points?

Building a Community

- Who needs money when you have friends?
- Conferences
- Summits (like this one!)
- Working Groups
- Your organization!

You’ve still got 98 other problems…

…but you’re not alone.

Questions?