RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: GPS2-R02

Threat Intelligence: Is it any good?

Guy Rosefelt

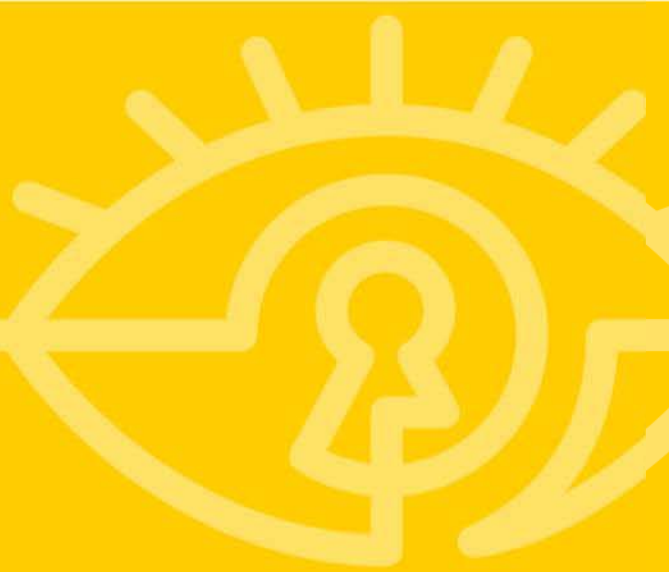
Dir, Threat Intelligence

NSFOCUS, INC

#RSAC

Agenda

- Why the bad rap?
- What is Threat Intelligence really?
- Why do we care?
- Some case studies that show value
- Some promising research
- How can you better apply Threat Intelligence?



Why the bad rap?

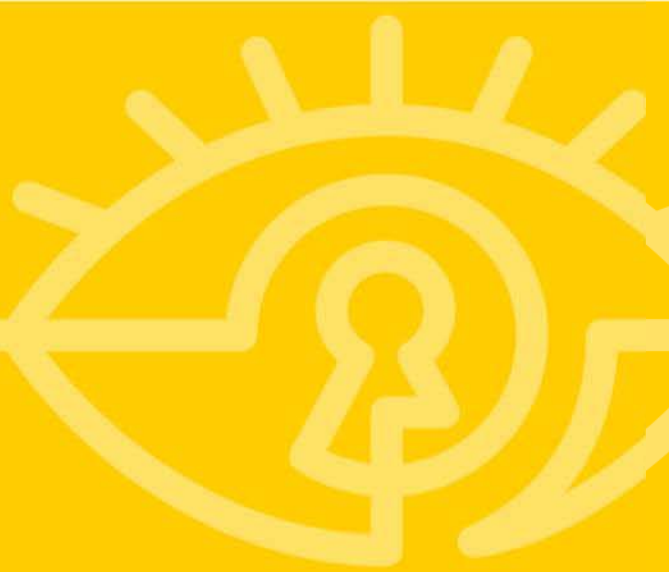
Implosion of Norse Corp

- **Sources: Security Firm Norse Corp. Imploding**
  - KrebsonSecurity – Jan 30, 2016
- **Norse Corp disappears shortly after CEO is asked to step down**
  - CSOOnline.com – Feb 01, 2016
- **Liar, Liar, KPMG Capital's Investment Into Norse Corp. On Fire**
  - Forbes – Feb 01, 2016
- **Fired Norse Corp CEO Blames the Media**
  - The Register UK – Feb 04, 2016

Cascade Effect

- **No, Norse is Not a Bellwether of the Threat Intel Industry but Does Hold Lessons Learned**
  - Robert M. Lee – Jan 30, 2016
- **Norse Is In Trouble-Just a company-specific blow, or raising bigger questions about threat intel.**
  - peerlyst – Jan 30, 2016

- **After Norse: VCs, pros eye cyber investments**
  - **SC Magazine –** Feb 3, 2016
- **Only 42% of infosec pros use threat intelligence, survey shows**
  - **Computer Weekly** – Mar 22, 2016
- **Threat Intelligence - The Answer to Threats or Another Fad?**
  - **Info security** – May 24, 2016



What is Threat Intelligence really?

Different Things to Different People

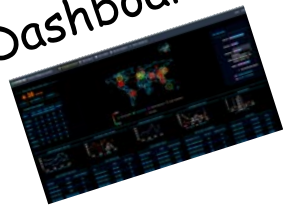
Data Feeds!

Auto NGFW/IPS/WAF Policy Creation

Correlation!

AV Signatures!

Dashboards!



CVE!

CWE!

Analyst Reports!

Gartner says…

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

-*Definition: Threat Intelligence , Gartner 16 May 2013*
(https://www.gartner.com/doc/2487216/definition-threat-intelligence)

Gartner says…

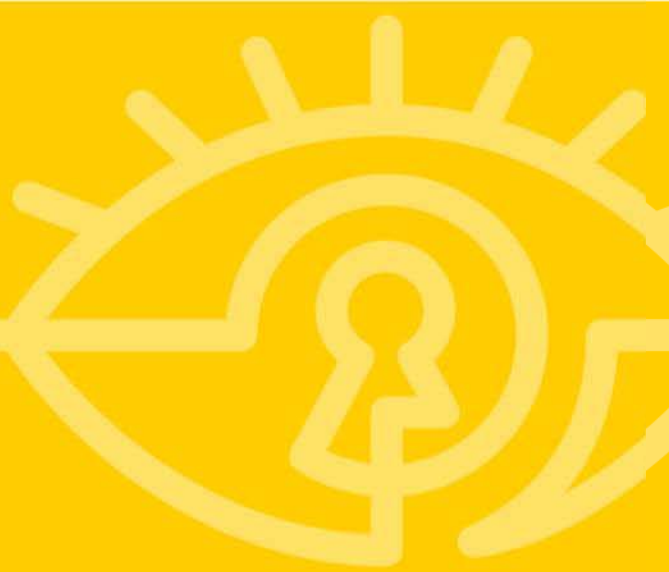
"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and ***actionable advice****, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."*

-Definition: Threat Intelligence , Gartner 16 May 2013
(https://www.gartner.com/doc/2487216/definition-threat-intelligence)

What is a Threat Intelligence Data Feed?

You might be surprised……

- Logs are your friend
  - WAF, IDS, web server, firewalls….
- You have your own curator
  - SEIM, log aggregator, Splunk…
- Open Source
  - Tons!... Hail a TAXII, I-Blocklist, OpenPhish Feeds, CVE database…
- Commercial
  - NSFOCUS, FireEye/iSight, Symantec, Cyveillance, …



Why do we care?

Threat Intelligence is what you do with it!

Buy a Subscription/Service ≠ Everything is Warm and Fuzzy

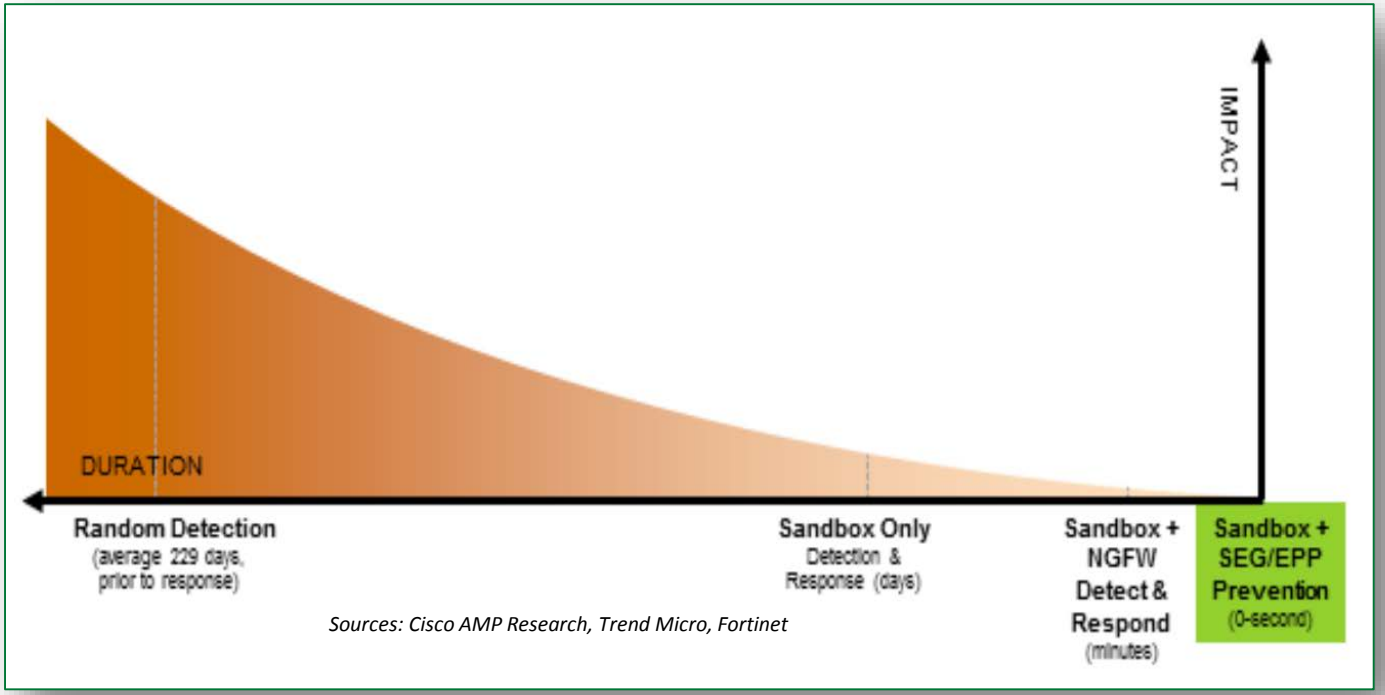
What do you want to do with it?

- Proactively block potential attacks
- Proactively block information leakage
- Detect threats faster
- Provide more context to security alerts
- Provide more context to vulnerabilities, exploits, etc.
- Provide better risk assessment about my internet presence, my organization, my industry, etc.

Reduce Time to Respond

Early Days Of Security

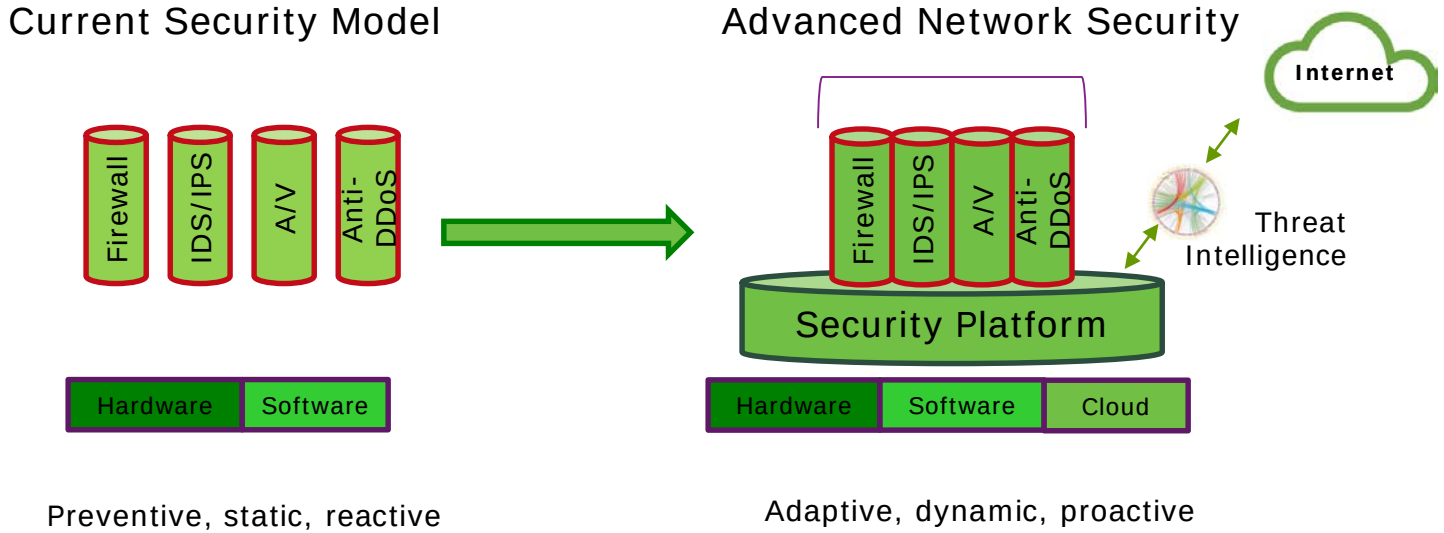
Detection Time vs. Impact



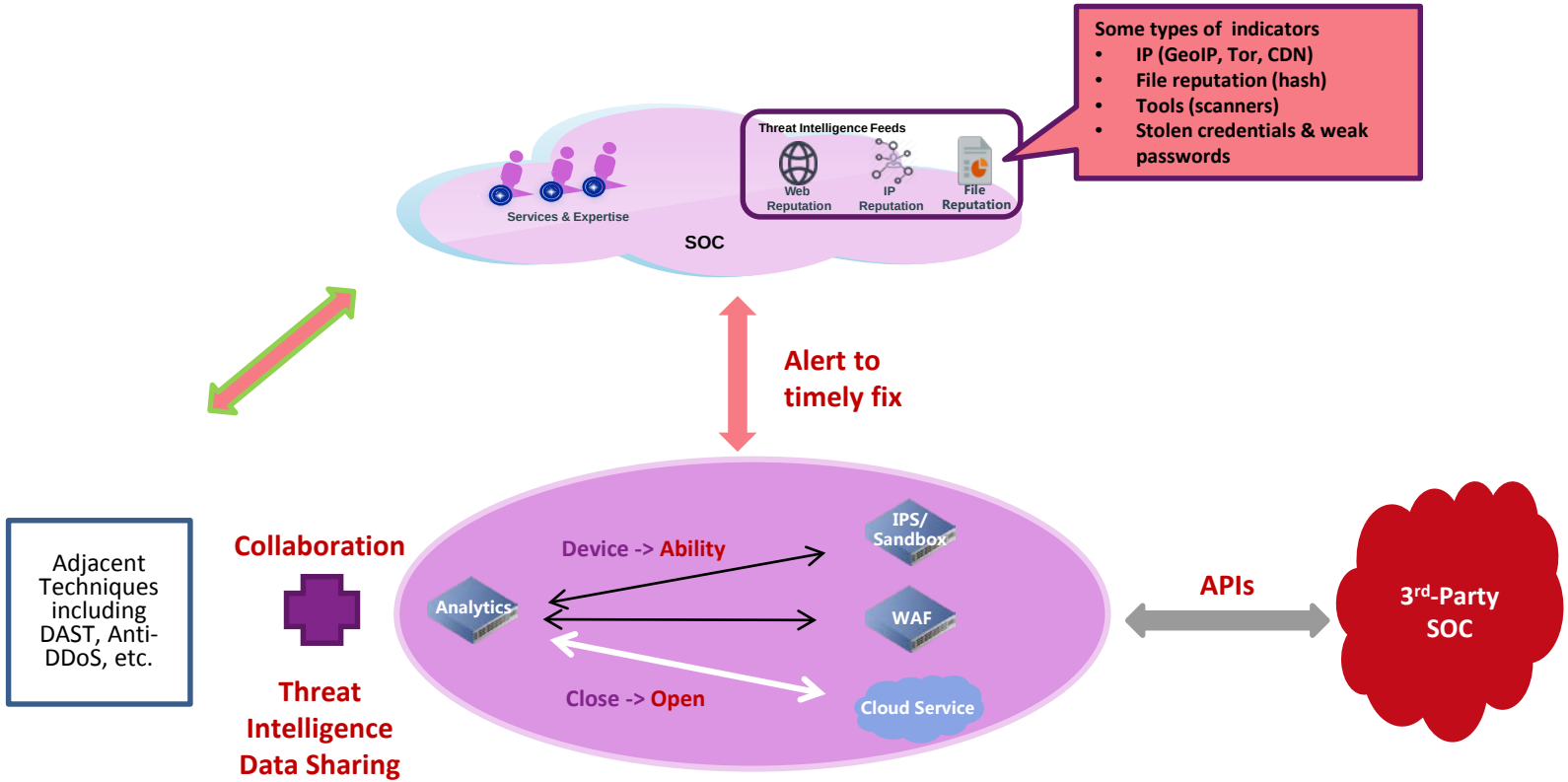
Sources: Cisco AMP Research, Trend Micro, Fortinet

Move to Share Data

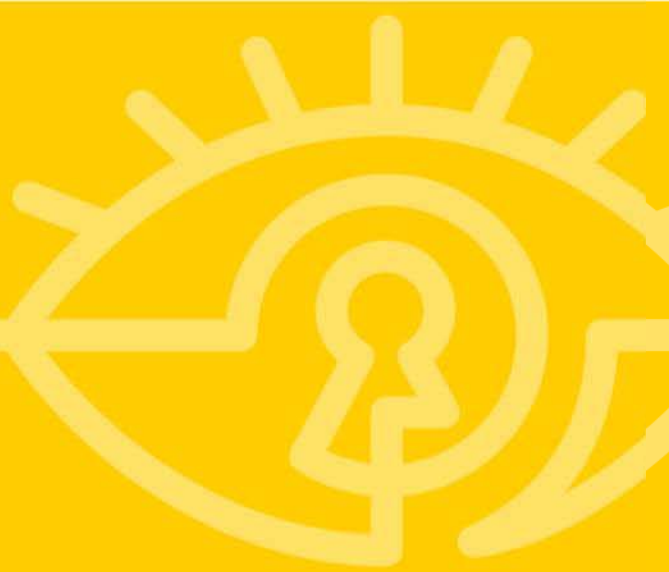
From Security Silos to a Security Platform



TI-driven Security Solution



Reduced Time to Prepare & Respond



Some case studies that show value

Case 1: Internet Assets Assessments

Customer: China ISP

Background: As an ISP provider, the customer has nearly a million IPs exposed to the internet. But, they lack a clear picture of their active IPs, ports, location, protocol, device types and versions of these internet assets, which usually brings great potential of risk to the owners.

Solution:

1. The ISP provides their following IP address fields for assessment, too large for common scanners to scan.

211.[redacted].*-211.[redacted].*
211.[redacted].*-211.[redacted].*
221.[redacted].*-221.[redacted].*
120.[redacted].*.*
120.[redacted].*.*
223.[redacted].*.*

2. Within 2 days, 13,899 of these IPs are found alive, and 64,335 ports are found open using an Internet of Things (IoT) search engine

Case 1: Internet Assets Assessments

3. The IoT portal identifies application services running on standard and non-standard ports. Even when some assets have changed their default ports, the right service can still be identified, with advanced non-standard port identification technology and enriched protocol fingerprint database.

4. IoT portal also acquires the banner information.

端口信息

445

SMB

server: WORKGROUP
os: Unix
lan manager: Samba 3.6.5
domain: WORKGROUP

	A	B	C	D	E
1	IP	Port	Protoc	Applic	Versio
2	223. 214	53	UDP	DNS	
3	223. .215	53	UDP	DNS	
4	223 .133	21	TCP	FTP	
5	223. .226	98	TCP	FTP	
6	223. .226	9029	TCP	FTP	
7	211. .184	21	TCP	HTTP	1.1
8	223. .10	22	TCP	HTTP	1.1
9	211 .171	23	TCP	HTTP	1.1
10	223. 242	6408	TCP	MEMCACHE	
11	223. .27	11211	TCP	MEMCACHE	
12	211. .126	20123	TCP	MYSQL	
13	211. .237	3306	TCP	MYSQL	
14	211. .236	20412	TCP	MYSQL	
15	223. .9	110	TCP	POP	
16	223. .5	995	SSL	POP	
17	223. .131	20110	TCP	POP	
18	223. .10	35000	UDP	RLOGIN	
19	211. .126	5351	UDP	RLOGIN	
20	211. .235	1099	TCP	RMI	
21	223. .9	10089	TCP	SSH	
22	223. .242	22	TCP	SSH	
23	223. .242	902	TCP	VMWARE	
24	223. 27	912	TCP	VMWARE	
25	223. .132	902	TCP	VMWARE	

Case 1: Internet Assets Assessments

5. By correlating with the geo-database, it can localize the IP asset.

ip 223.[redacted].214

China, Liaoning

6. By correlating with a reputation database, we identified whether the IP addresses are listed in the blacklist with malicious behaviors.

IP	Malicioius Type	Detected Date
199.[redacted].169	exploit	2016-07-10
31.[redacted].200	bots	2016-07-10
85.[redacted]89	scanner	2016-07-10
78.[redacted].238	ssh	2016-07-10
143.[redacted]83	scanner	2016-07-10
211.[redacted].36	ssh	2016-07-10
91.[redacted]206	scanner	2016-07-10

Case 1: Internet Assets Assessments

8. Using reverse DNS functionality, we get the domain names correlated with the IP.

9. By extracting the title information of the website, it shows the business that the website runs.

IP*	Country*	Provice*	City*	Port*	Service*	URL	Name of the System
222.[redacted].140	China	Fujian	Fuzhou	80	http	http://222.[redacted]140/	10000管家 - 中国电信
219.1[redacted].77	China	Beijing	Beijing	80	http	http://219.1[redacted]2.77/	电信-终端管理
222.[redacted].215	China	Neimenggu	Huhehaote	80	http	http://222.[redacted].215/	电信-3G下载平台

Case 2: Investigation of Unknown Threats

Background

During the regular check, the security administrator found several hosts in the testing environment were infected with worm virus. Upon further analysis, the security officer discovered these infected assets all outreached to six groups of suspicious Command & Control domains.

Solution

Using IoT portal and forensics helps to dig further into unknown threats.

Case 2: Investigation of Unknown Threats

Solution

IoT portal helps to dig further into unknown threats

1. Analyze the suspicious domains using IoT portal to explore the IP addresses that hosted these domains. Take one of these groups as an example:

2. These four IPs are all correlated with malware.

3. These domains are registered by the same registrant and email-box

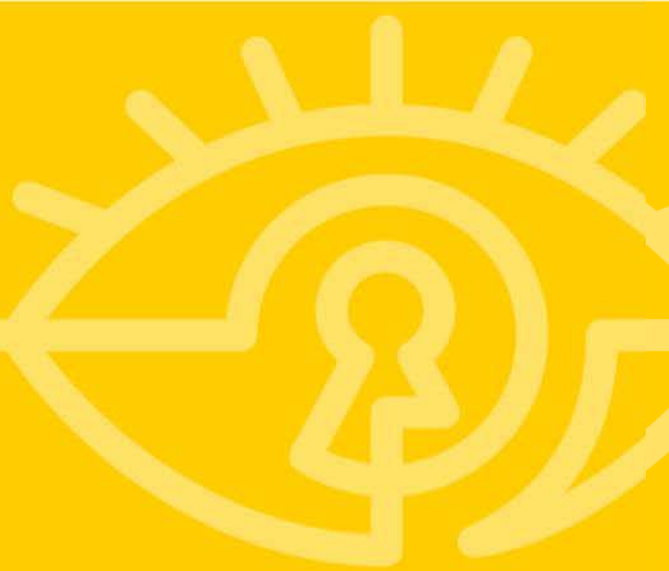
Case 2: Investigation of Unknown Threats

Solution

IoT portal helps to dig further into unknown threats

4. This email-box has also registered the other 1458 domains.

5. These 1458 domains all resolved to the same IP as listed in 1. And 99.6% of these domains are registered in less than one year. 1456 of these domains are still effective. All of these active domains and the registration email-boxes are filed to the NTI intelligence blacklist for further tracking.



Some promising research

DNS Big Data Mining

There are a lot of interesting patterns that can be found from analyzing large sets of DNS queries

- Detection Based on the Characteristic of Periodic Communication
- Detection Based on the Characteristic of Random Domain Names

Detection Based on the Characteristic of Periodic Communication

- Most HTTP botnets are can be identified by periodic communication.
- These botnets communicate with C&C hosts and initiate DNS requests at fixed intervals.
- Using "Shangxing Remote Control" as an example
  - When accessing C&C hosts via domain names, it initiates a DNS query request every 60 or 1800 seconds.

Detection Based on the Characteristic of Random Domain Names

- **Domain generation algorithms** (DGA) are algorithms found in families of malware used to periodically generate a large number of domain names that can be used as connection points with command & control servers
- DGA-generated domain names have several lexical characteristics, such as probability distribution of character frequency, strong randomness in character combinations, string lengths, and the number of dots
- Valid domain names are easy to pronounce with alternating vowels and consonants, while DGA-generated domain names may have consecutive consonants.
- The analysis of "strange" domain names can help detect botnets.

How can you better apply Threat Intelligence?

What do you want to do with it?

- Proactively block potential attacks
- Proactively block information leakage
- Detect threats faster
- Provide more context to security alerts
- Provide more context to vulnerabilities, exploits, etc.
- Provide better risk assessment about my internet presence, my organization, my industry, etc.

How can you better apply Threat Intelligence when you get home?

- Look around you
  - Take stock of where you aggregate data
    - Syslog servers
    - SEIMS
    - System and Web scanners
  - Take stock of information sources you receive
    - Newsfeeds
    - Email alerts
    - Podcasts (SANS, McAfee, etc.)

How can you better apply Threat Intelligence when you get home?

- Do your data sources provide context information about vulnerabilities and exploits relevant to your environment?
  - Can you automatically or manually capture that information into a file?
- Do any of your security products have the ability to accept TI feeds directly?
  - Enable access
    - Start trial subscription if commercial (paid) service
  - Is there an API you can use to upload context information you have identified?

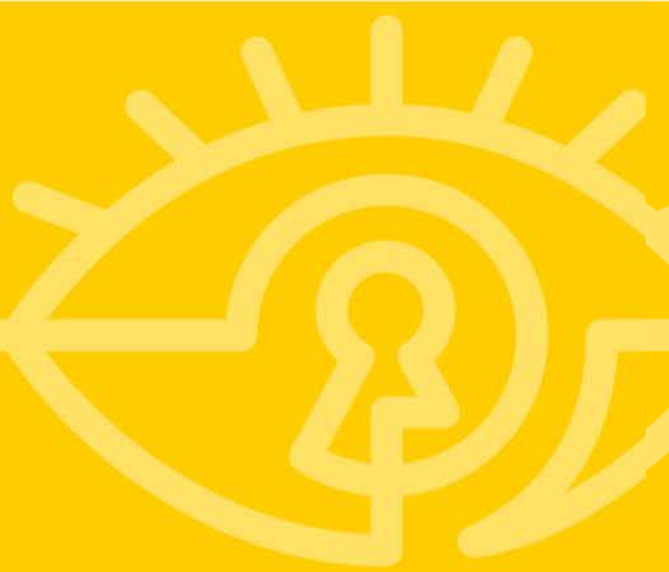
How can you better apply Threat Intelligence in the next 30 days?

- Research and subscribe to open source feeds relevant to you
  - SHODAN, CVE Database, The Defense Cyber Crime Center (DC3), European Union Agency for Network & Information Security (ENISA)
  - Use this data to provide additional context to alerts, vulnerability scans, SEIM, etc.
- Get access to asset management data
  - Understand what key or business critical assets there are
  - This will help prioritize patch and vulnerability remediation planning
- Both of the above can improve or help design metrics
  - Remediation
  - Incident response

How can you better apply Threat Intelligence in the next 90 days?

- Research and evaluate commercial feeds relevant to you
  - From your security vendor, 3rd parties, etc.
  - Use this data to provide additional context to alerts, vulnerability scans, SEIM, etc.
- Research and evaluate risk assessment/vulnerability management tools
  - Open source or commercial
  - Automate patch remediation prioritization and planning
  - Makes use of key or business critical assets you identified
- Both of the above can improve or help design metrics
  - Remediation
  - Incident response

Reduced Time to Prepare & Respond



Thank you!