RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: AIR-W12

THREAT INTEL AND CONTENT CURATION: ORGANIZING THE PATH TO SUCCESSFUL DETECTION

Justin Monti

CTO
MKACyber

Mischel Kwon

CEO
MKACyber
@MKACyber

What is Cyber Threat Intelligence

Data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators

Commonly lists of atomic indicators – IP addresses, hostnames, file hashes – associated with malicious activity

Significant push to increase sharing of this intel

- U.S. Gov CISA legislation and proposed CISPA
- DHS AIS program to increase indicator sharing among federal entities
- Numerous ISACs deploying machine readable/automated indicator exchanges
- Most major security tool vendors provide some sort of threat feed offering with their product
- OASIS, IETF and other standards initiatives

Cyber Threat Intel - Sources

Open Source
Internet lists, blogs, GitHub repositories – often maintained by a community with highly variable levels of review/vetting of submitted IOCs.

Commercial
Intelligence sold as a product or a feature of a product/service. Varies from aggregated open source intel to sophisticated reporting on threat actors. MSSP providers are often able to aggregate observations from across their customer base into intel products.

Government
Intelligence provided to protect National assets and critical infrastructure. DHS NCCIC, Sector-specific agencies (e.g. HHS for Healthcare, DoE for Energy, DoD for Defense, FAA for Aviation).

Internal
Intel specific to your organization based on observed events and knowledge of personnel, business structure, IT architecture and industry.

Threat Report – source for intel

Microsoft Office Vulnerabilities Used to Distribute Zyklon Malware in Recent Campaign

January 17, 2018 | by Swapnil Patil, Yogesh Londhe

Introduction

FireEye researchers recently observed threat actors leveraging relatively
HTTP malware. Zyklon has been observed in the wild since early 2016 a

Zyklon is a publicly available, full-featured backdoor capable of keyloggir
additional plugins, conducting distributed denial-of-service (DDoS) attack
communicate with its command and control (C2) server over The Onion
can download several plugins, some of which include features such as c
browsers and email software. Zyklon also provides a very efficient mecha

Infection Techniques

CVE-2017-8759

This vulnerability was discovered by FireEye in September 2017, and it is a vulnerability we have observed being exploited in the wild.

The DOC file contains an embedded OLE Object that, upon execution, triggers the download of an additional DOC file from the stored URL (seen in Figure 3).

```
09 00 0D 00 0A 00 09 00 0D 00 0A 00 48 00 74 00  ............H.t.
54 00 50 00 3A 00 2F 00 2F 00 32 00 35 00 38 00  T.P.:././.2.5.8.
34 00 37 00 36 00 33 00 38 00 33 00 30 00 3A 00  4.7.6.3.8.3.0.:.
38 00 30 00 30 00 32 00 2F 00 61 00 75 00 63 00  8.0.0.2./.a.u.c.
2F 00 64 00 6F 00 63 00 2E 00 74 00 78 00 74 00  /.d.o.c...t.x.t.
```

Figure 3: Embedded URL in OLE object

CVE-2017-11882

Similarly, we have also observed actors leveraging another recently discovered vulnerability (CVE-2017-11882) in Microsoft Office. Upon opening the malicious DOC attachment, an additional download is triggered from a stored URL within an embedded OLE Object (seen in Figure 4).

Threat Intel Example – Raw Indicators

Indicators of Compromise

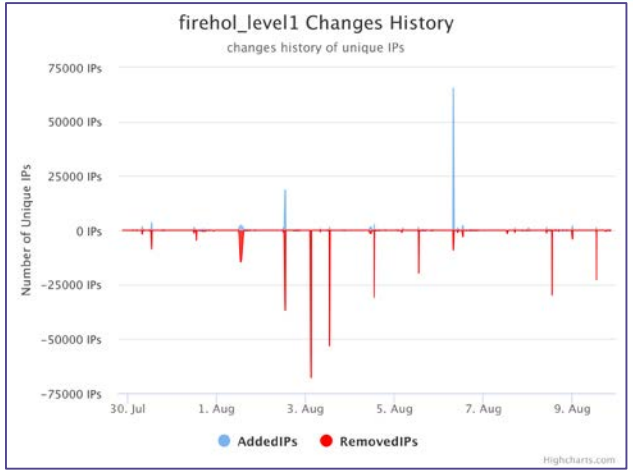
The contained analysis is based on the representative sample lures shown in Table 3.

MD5	Name
76011037410d031aa41e5d381909f9ce	accounts.doc
4bae7fb819761a7ac8326baf8d8eb6ab	Courrier.doc
eb5fa454ab42c8aec443ba8b8c97339b	doc.doc
886a4da306e019aa0ad3a03524b02a1c	Pause.ps1
04077ecbdc412d6d87fc21e4b3a4d088	words.exe

Network Indicators

- 154.16.93.182
- 85.214.136.179
- 178.254.21.218
- 159.203.42.107
- 217.12.223.216
- 138.201.143.186

Challenge – Too Much Intel

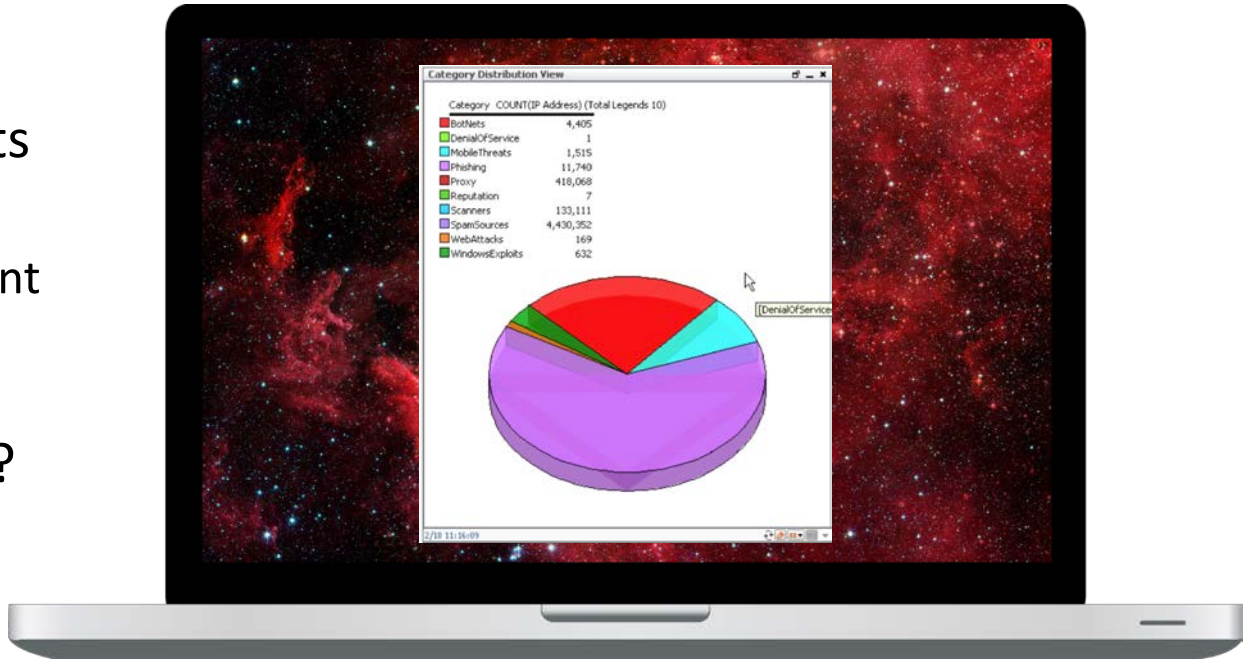


Total of 652M unique IPs in this feed!

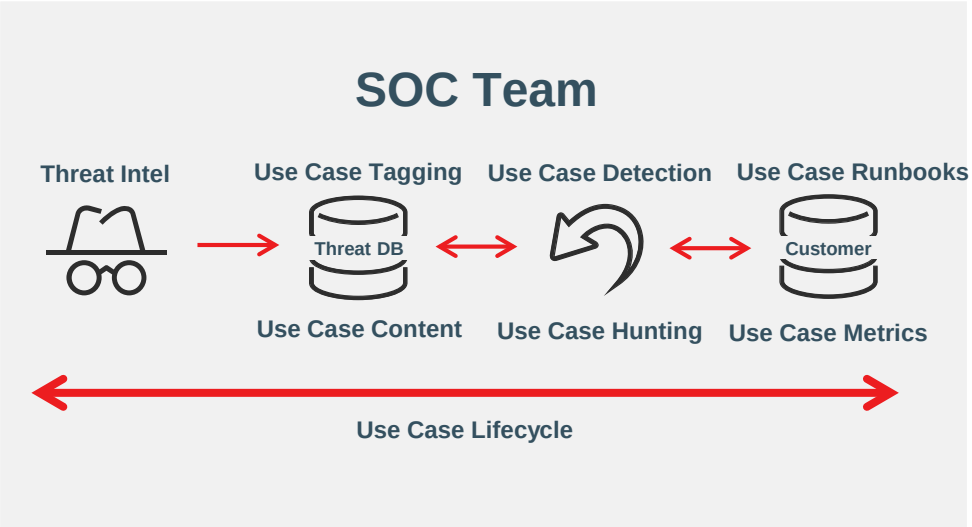
- Billions of atomic indicators
- Invalid data
- No indication of severity
- Often disconnected from campaign
- More indicators lead to more alerts
- Lead to Analyst alert fatigue
- No prioritization

Analyst Fatigue from Indiscriminate Feed Ingestion

- Too many hits
- What should analysts investigate?
  - No Use Case alignment
- Priority?
- Risk to organization?



Use Case Methodology



- Use Case methodology drives SOC **detection and hunting**
- Leverages **tagged and curated** threat intel and tool content
- Ensures analysts are **aligned to risk priorities** in defending the enterprise

Management is key –

driving the intentional selection of relevant intel, aligning with use cases and applying to the security architecture.

Solution – Threat Intel Management Process

What to consume?

- Linked to protecting the business
- Correlated to vulnerability (CVE)
- Aligned to organization's security architecture

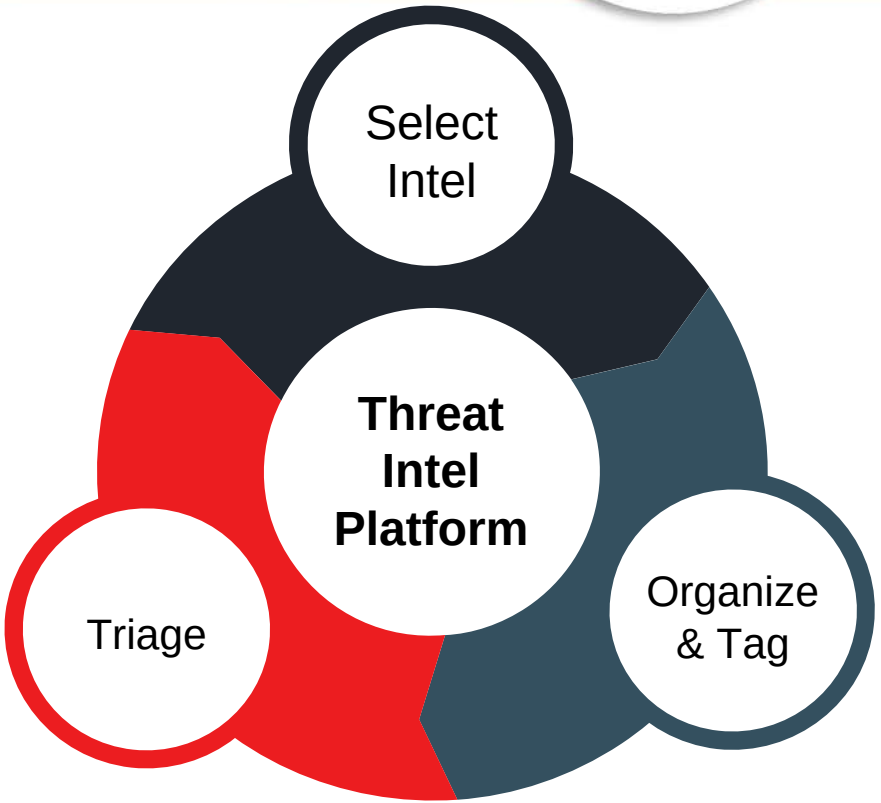
How to organize it?

- Link to Use Case
- Link back to source reporting
- Link to Content through Content Curation process

Triage and Content Curation

- De-duplication of IOCs across sources
- Regular review
- Remove stale/noisy IOCs

All supported by a Technology Platform



Threat Modeling = Risk Prioritization

- Business Threat
- Insider Treat
- Customer Threat
- Hygiene

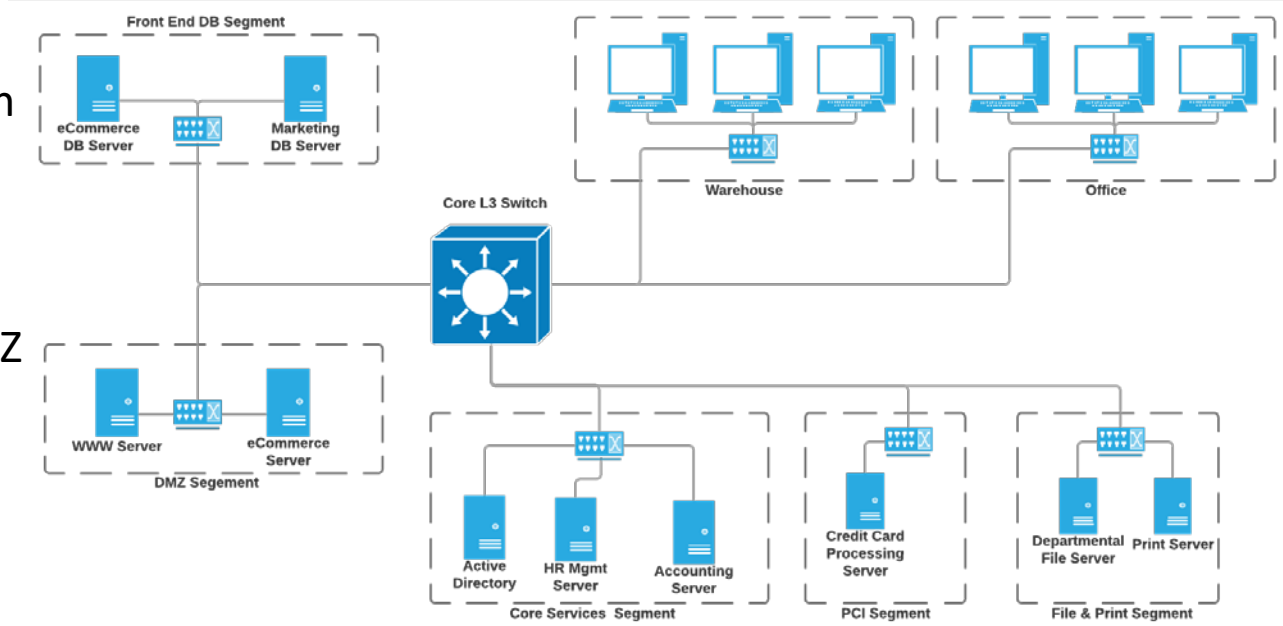
- Assets
- Architecture
- Applications
- DB/Datastore

- Prioritize **threat intel** by risk to business
- Requires **understanding risks** of concern to business
- Requires **sound inventory** of systems, assets, applications
- Understanding **hygiene** state of the environment
- All captured in a threat modeling capability to surface **the highest priority risks**
- Apply threat intel **aligned to use cases** to help address these risks

mka cyber

Apply Intel Where Relevant

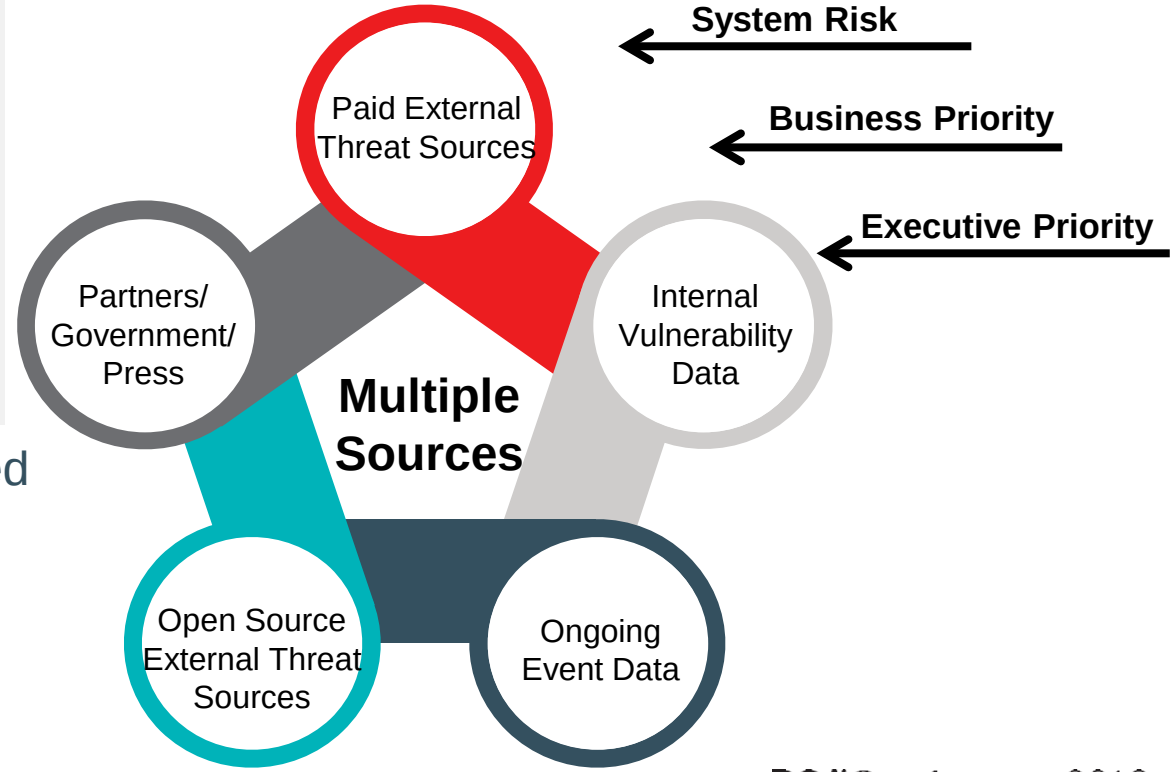
- Network segments – align with threat
  - Opportunistic malware in the user segment – workstations most likely target
  - Exploits for server vulnerabilities in the DMZ
  - Targeted attacks in the network core – server and sensitive data enclaves – identity/authentication providers



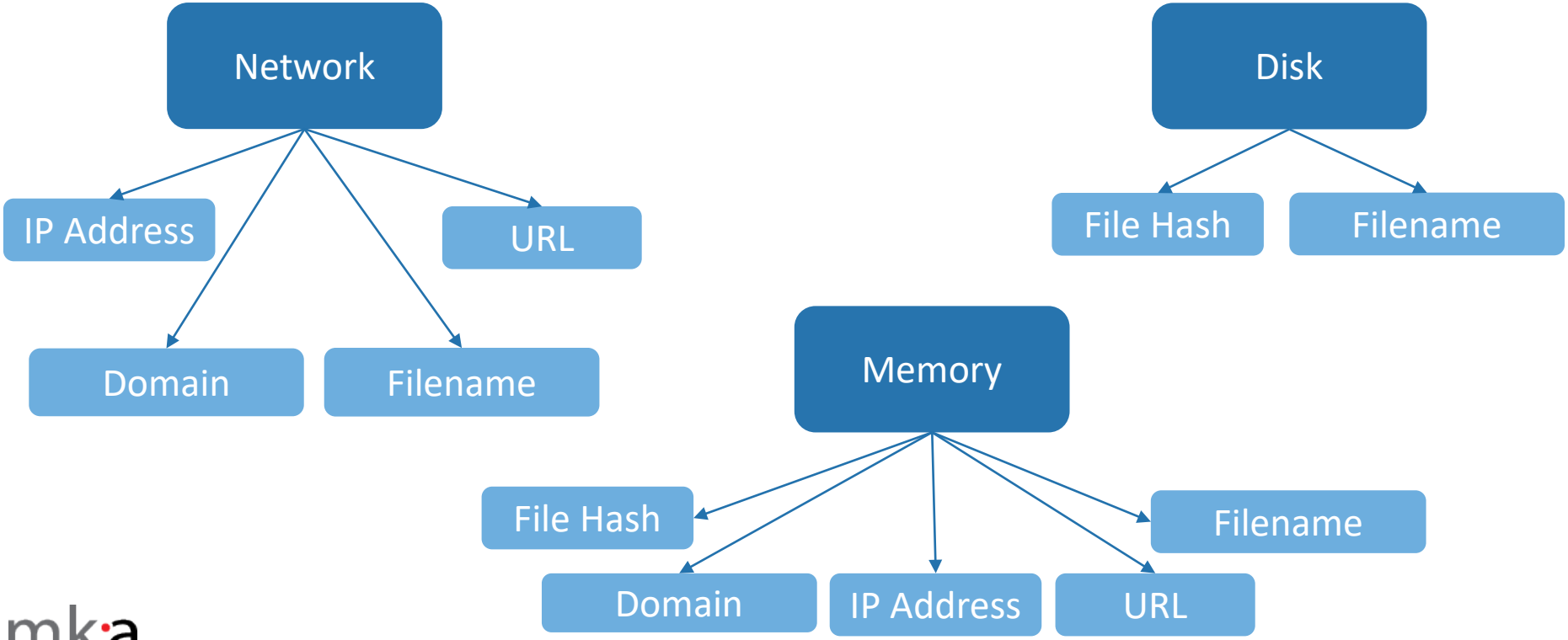
Threat Source Selection and Drivers

- Focus on Business Risk
- Avoid nuisance malware distractions
- Ensure SOC visibility across enterprise

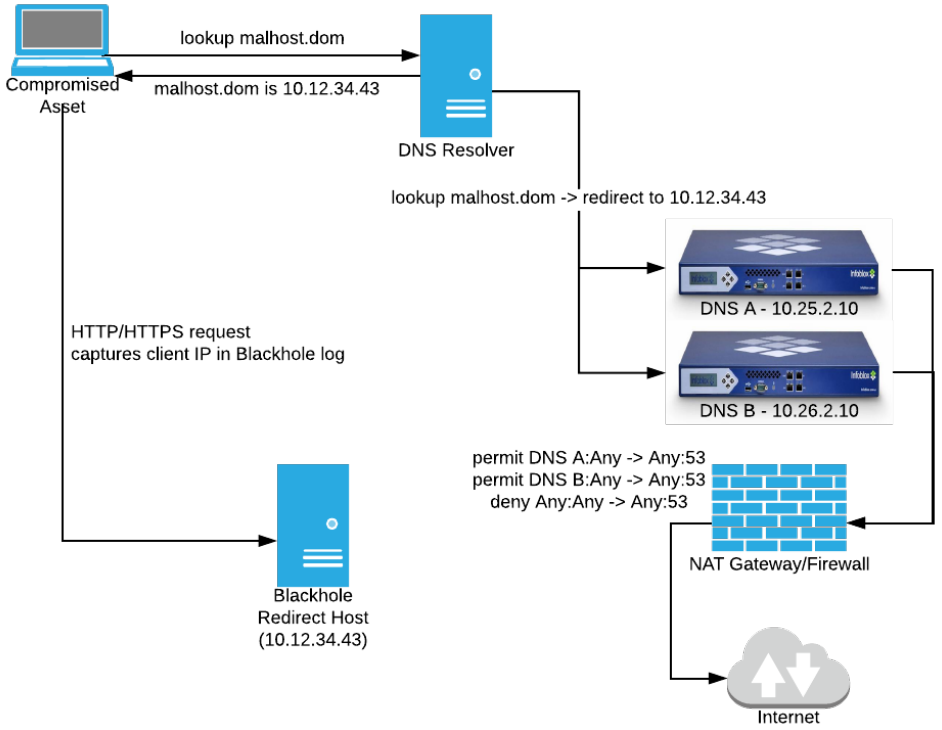
Goal: SOC and analysts focused on threats presenting greatest risk to the business mission



Hunting Produces Internal Intelligence – Sources & Indicators



DNS Blackhole – Internal Intel Source




```
{
 "timestamp": "2018-02-13 02:04:28.039752 +0000 UTC",
 "bytes_client": "86",
 "http_method": "GET",
 "url_path": "/Fb3De8/pown.php",
 "http_version": "HTTP/1.1",
 "http_user_agent": "curl/7.54.0",
 "dst_name": "it.support4u.pl",
 "src_ip": "192.168.58.1",
 "src_port": "58692",
 "sinkhole_instance": "netsarlacc-blackhole",
 "sinkhole_app": "http",
 "sinkhole_tls": false,
 "request_error": false
}
```


Cisco CSIRT netsarlacc - https://github.com/ciscocsirt/netsarlacc

Evaluate Threat Feed Value

Define Threats	Executive leadership identifies potential threats specific to organizational goals and risk
Quantify Risk	Prioritize identified threats Impact (I) x Probability (P) = Risk (R)
Identify Data Feeds	Primary data feeds that provide detection and analysis value for identified threats
Narrow Focus	Validate data feeds against actual activity observed in organization Remove feeds which do not align with SOC tooling or visibility
Monitor/Adjust	Enrich Intel with observed events and incidents Adjust feeds, sources, content based on analyst feedback

Threat Intel Feedback Loop

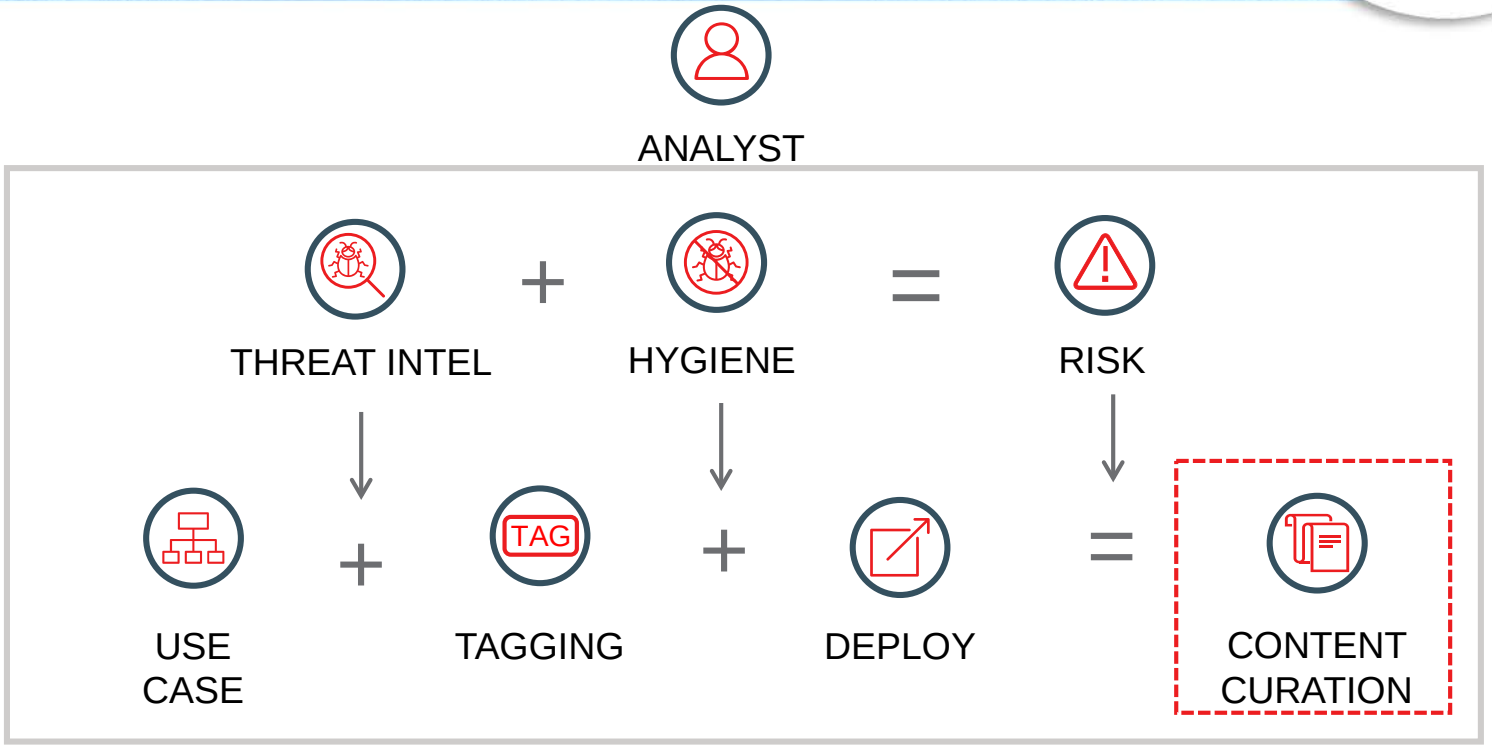
- Not set it and forget it
- Requires feedback from analysts
- Clear out the garbage
- Tune content with new intel
- Analysis surfaces new indicators – potentially related via campaigns
- Capture this internally generated intel – valuable!

- Detection Content
- Drives Analysis & Investigations

- Enriches Threat Data
- Prioritize Activities – both detection and remediation

mk·a cyber

Threat Methodology



Threat Intel Example - Tagging and Organizing

Raw Indicators

Indicators of Compromise

The contained analysis is based on the representative sample lures shown in Table 3.

MD5	Name
76011037410d031aa41e5d381909f9ce	accounts.doc
4bae7fb819761a7ac8326baf8d8eb6ab	Courrier.doc
eb5fa454ab42c8aec443ba8b8c97339b	doc.doc
886a4da306e019aa0ad3a	
04077ecbdc412d6d87fc2	

Network Indicators

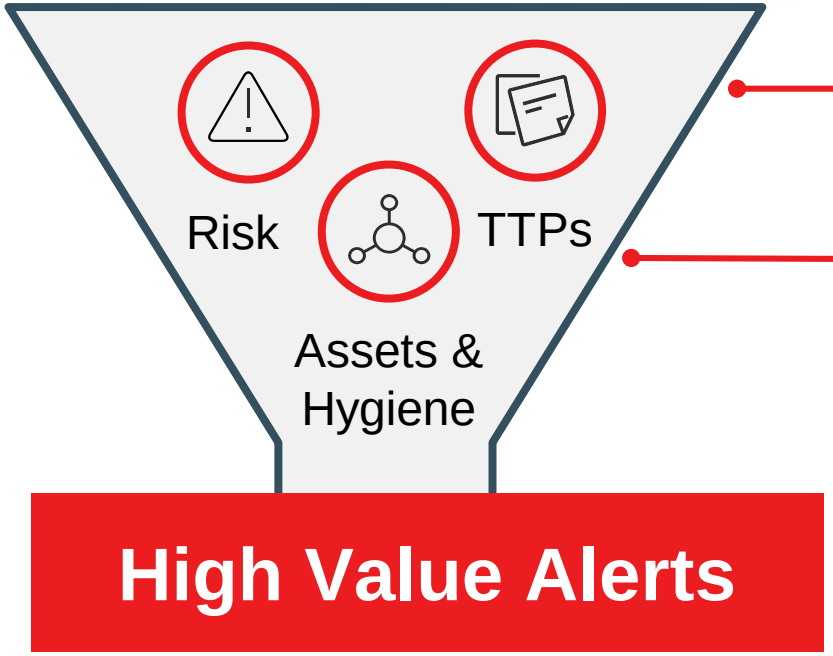
- 154.16.93.182
- 85.214.136.179
- 178.254.21.218
- 159.203.42.107
- 217.12.223.216
- 138.201.143.186

Tagged and Organized

IOC	Type	CVE	Source	Use Case
Accounts.doc	File	CVE-2017-8759 CVE-2017-11882	FireEye www....	Phishing
Doc.doc	File	CVE-2017-8759 CVE-2017-11882	FireEye www....	Phishing
159.203.42.107	IP	CVE-2017-8759 CVE-2017-11882	FireEye www....	Phishing
TOR network use	TTP		FireEye www....	Malware

mka cyber

Driving High Value Alerts



Understand Business Risk Priorities

Understand threat information, monitoring processes, and system status

Use Case methodology aligns alerts to use cases ensuring that analysts cover all detection scenarios and stay focused – not chasing shiny objects.

Content Development

DNS Blackhole

```
warnono.punkdns.top IN  A 192.168.0.1  ;Threat ID 24158 - phishing
```

IDS Signature

```
alert ip any -> 159.203.42.107 any (
msg:"UC\=Phishing\;ThreatID\=24158"; priority:1; )
```

SIEM Signature (output would be displayed in Phishing channel/dashboard)

```
index="bro" sourcetype="bro_conn" 159.203.42.107 OR
warnono.punkdns.top
```

Threat Intel Spreadsheet

- Analyst review of IOCs
- Tagged to:
  - Attack
  - Report
  - Use Case and Scenario
- Dates tracked to facilitate Content Curation process

ID	IOC	Type	Source Ni-Ti	Source Report	Publish Date	Run Date	Use Case	Scenario	Attack Compone
234816080	cc89ddac1afe69069eb18bac58c6a9e4	MD5	Open Source	https://fireeye.com/bl	7/14/17	7/14/17	Malware	Hosts infected with malware	
234816080	cc89ddac1afe69069eb18bac58c6a9e4	MD5	Open Source	https://fireeye.com/bl	7/14/17	7/14/17	Malware	Malicious link	
234843418	89.223.26.20	IP	Open Source	https://zeustracker.ab	7/14/17	7/14/17	Malware	Hosts infected with malware	
235007467	it.support4u.pl	Domain	Open Source	https://threatpost.com	7/14/17	7/14/17	Malware	Hosts infected with malware	Malware Execution
271345255	www.oguhtell.ch	Domain	Open Source	http://blog.trendmicr	12/1/16	8/3/17	Data Exfil	Unusual large Upload	Command and Control (C2)
271372639	Http://wok.com	URL	Open Source	Isitworking.com	8/4/17	8/4/17	Data Exfil	Unusual Network Session lengths	
271536963	hxxp://jbrianwashman.com/images/photo26962/main.ph	URL	Open Source	http://blog.trendmicr	12/1/16	12/1/16	Email Monitoring	Email Volume Spike	
271619139	ribotqtonut.com	Domain	Open Source	https://securelist.com/	8/15/17	8/15/17	Traffic anomalies/Stats	IOC/Intel Content Match	
271728721	getmyfiles@keemail.me	Email	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271756119	getmyfiles@scryptmail.com	Email	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271783518	getmyfiles@mail2tor.com	Email	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271810918	image.ibb.co	Domain	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271838319	sm.uploads.im	Domain	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271865721	185.10.202.115	IP	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271893124	https://image.ibb.co/mxRqXF/arrival.jpg	URL	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
271920528	http://185.10.202.115/images/arrival.jpg	URL	Open Source	https://www.bleeping	8/16/17	8/16/17	Malware	Hosts possibly infected with ransomware	
272030154	267f144d771b4e2832798485108decd505cb824a	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	
272084973	http://46.183.165.45:80/imageload.cgi	URL	Open Source	MKAC Threat Research	8/29/17	7/7/17	Traffic anomalies/Stats	IOC/Intel Content Match	
272112384	verdadeoumito.com	Domain	Open Source	MKAC Threat Research	8/29/17	6/21/17	Traffic anomalies/Stats	IOC/Intel Content Match	
272139796	23f1e3be3175d49e7b262cd88cfd517694dcba18	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	Malware Download
272222038	kuessnermalt.de	Domain	Open Source	MKAC Threat Research	8/29/17	6/25/17	Traffic anomalies/Stats	IOC/Intel Content Match	
272249454	4701828dee543b994ed2578b9e0d3991f22bd827	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	
272276871	sender@grupofreitas.ltda	Email	Open Source	http://www.malware-	10/7/17	10/6/17	Email Monitoring	Phishing link	
272331708	228da957a9ed661e17e00efba8e923fd17fae054	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	
272359128	411ef895fe8dd4e040e8bf4048f4327f917e5724	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	Malware Download
272413971	www.petr4.in	Domain	Open Source	http://www.malware-	10/7/17	10/6/17	Malware	Hosts infected with malware	
272441394	bd194a81bfed3d57744183dd700e9e4a68f7b05b0f4c94a4	SHA256	Open Source	http://www.malware-	10/7/17	10/6/17	Malware	Hosts infected with malware	
272496243	11b35320fb1cf21d2e57770d8d8b237eb4330eaa	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	Malware Download
272523669	22542a3245d52b7bcdb3eaef5b8b2693f451f497	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	Malware Download
272551096	2b9faa8b0fcadac710c7b2b93d492ff1028b5291	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	Malware Download
272578524	3944253f6b7019eed496fad756f4651be0e282b4	SHA1	Open Source	https://www.welivese	8/30/17	8/30/17	Malware	Hosts infected with malware	
272770548	71.83.124.6	IP	Open Source	MKAC Threat Research	8/29/17	6/11/17	Traffic anomalies/Stats	IOC/Intel Content Match	Ransomware/Crimeware
272825421	valforte.com	Domain	Open Source	MKAC Threat Research	8/29/17	6/22/17	Traffic anomalies/Stats	IOC/Intel Content Match	Ransomware/Crimeware

Curated Content

IOC	Use Case	Scenario	Data Source Required	Action	Tool	Content
flexberry.com	Malware	Hosts infected with malware	• IDS • Firewall	Block Detect	Blackhole Splunk	zone "flexberry.com" IN {type master; file "blackhole.zone"; index=stream sourcetype=stream:http host="flexberry.com" | stats count by src
http://proxyholding.com/Information/	E-mail	Phishing/Malicious link	• Email • Firewall	Block Detect	Blackhole Splunk	zone "proxyholding.com" IN {type master; file "blackhole.zone"; index=stream sourcetype=stream:http dest_port=80 host="proxyholding.com" url="Information/*" | stats count by src
94.130.210.177	Malware	Post infection C2 beaconing	• IDS • Firewall	Detect Block	Splunk Palo Alto	index=cisco dest_ip=94.130.210.177 | stats count by src <destination> <member>94.130.210.177</member> </destination>
ps://bankosantantder.com/applet_signed.	Malware	Hosts infected with malware	• IDS • Firewall	Detect Block	Splunk Blackhole	index=stream sourcetype=stream:http dest_port=443 host="bankosantantder.com" url="*applet_signed.jar" | stats count by src zone "bankosantantder.com" IN {type master; file "blackhole.zone";
ttp://vanuffelen.net/Outstanding-Invoices	E-mail	Phishing/Malicious link	• Email • Firewall	Detect Block	Splunk Blackhole	index=stream sourcetype=stream:http dest_port=80 host="vanuffelen.net" url="Outstanding-Invoices/*" | stats count by src zone "vanuffelen.net" IN {type master; file "blackhole.zone";
ttp://weselnegrajki.pl/Outstanding-Invoices	E-mail	Phishing/Malicious link	• Email • Firewall	Detect Block	Splunk Blackhole	index=stream sourcetype=stream:http dest_port=80 host="weselnegrajki.pl" url="Outstanding-Invoices/*" | stats count by src zone "weselnegrajki.pl" IN {type master; file "blackhole.zone";
d5d62229f5ec54f49dde792b27c09300	DMZ	Web Shell Detected	• Public facing webapp logs (IIS/Apache,	Detect Block	Splunk Tanium	index=bro sourcetype=bro_file md5="d5d62229f5ec54f49dde792b27c09300" | stats count by src d5d62229f5ec54f49dde792b27c09300
tcp://xm4:x@178.170.189.193:82	DMZ	Successful Web application attack	• Public facing webapp logs (IIS/Apache,	Detect Block	splunk Palo Alto	index=cisco proto=tcp dest_ip=178.170.189.193 dest_port=82 | stats count by src <destination> <member>178.170.189.193</member> </destination>
3|00|A|00|_|00|P|00|R|00|O|00|J|00|E|00	Malware	Host Infected With Malware	• Windows Events (System) • A/V or other endpoint security	Detect	Snort	alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT SUSPICIOUS Possible Office Doc with Embedded VBA Project (Wide)"; flow:established,from_server; flowbits:isset,et.MCOTT; file_data; content:" |00|V|00|B|00|A|00| |00|P|00|R|00|O|00|J|00|E|00|C|00|T|00|"; nocase; flowbits:set,et.DocVBAProject; classtype:bad-unknown; sid:2019837; rev:2;)

Content developed to detect (reactive) and block (proactive) activity associated with threat intel indicators is tagged to use case/scenario and associated with required data source and tool

mka cyber

RSAConference2018

Summary

Analyst review, tagging and Content Curation are the **path to success!**

- Collecting Threat Intel Feeds just to have more feeds hurts the SOC
  - Analyst Fatigue
  - Irrelevant Alerts
  - Noise
- Threat Intel must be soundly managed as part of an overall SOC methodology
  - Understand Business Risk to focus on relevant threat intel sources
  - Prioritize based on threat modeling and understanding the environment

Putting It Into Action

- Review your threat model – what attack vectors are most likely?
  - This will guide you to Use Case Selection
- Review your Threat Intelligence – is it giving you relevant and actionable information for your Use Cases and Tooling?
  - Eliminate sources that don't align
  - Begin tagging content generated from Threat Intel
- Track your Threat Intel and Content
  - Spreadsheets can work in a pinch
  - Look at deploying a threat intel management tool
- Capture analyst feedback to continually improve and curate the Threat Intel and Content