Threat Intel for All:
There’s More to Your Data than Meets the Eye

By @3ncrepted
07/28/2017  Wall of Sheep
Cheryl Biswas

- Security consultant researcher/analyst in Threat Intel.
- Loves APTs, mainframes, ICS SCADA & creating security awareness
- StarTrek! Boldly Go!
- The Diana Initiative
- Specialised honours degree in political science
- ITIL designation
- Talks: BSidesLV, Circle City, BSidesT0, SecTor, Hackfest, InteropITX
- Writer and blogger
- @3ncr1pt3d
Disclaimer

The views and opinions expressed herein are those of the presenter and do not represent those of any employer, past or present.

As well, any product or company mentioned is solely for illustrative purposes and not as an endorsement.
Agenda

- Threat Intel 101: From Buzzword to Keywords
- Create a Baseline: Know Thyself
- Care & Feeding of Your Data
- Analysis: Threat Correlation
- Target takes Aim: Flip the table
- Conclusion & Recap
What is your data doing for you?

Threat Intel 101
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.

Gartner
There are all kinds of people in your neighbourhood
Understanding Threat Intel

- Situational Awareness
- Data does not equal intelligence
- New threats need new approaches: DGA
- No one tool does it all
- Move beyond the perimeter
- Use what you have – Moar is not better
- False positives
Key Points to Consider

- “Finished Intelligence” – data made to measure for you
- Go for good, not great. Get it up and running
- Opportunity, Capability, Intent – make it relevant
- Threat Intel Fusion points
- Objectives: become proactive
Context

- History
- Patterns
- Anomalies
Relevance

Yes, but what does this mean to you?
There is no more relevant threat intelligence than what is actually occurring within your organization

Rick Holland, Forrester Research
Objective

Go for *good*, not great.
You just want to get going.
Visibility

Are you seeing *all* there is to see?
Per RSA: Since threat actors change their tools and techniques, threat intelligence has a shelf life. That means security teams need to be armed with great visibility and a variety of current source of threat data to bring the attacks into view.

What is your data doing for you?

Create a Baseline: Know Thyself
Why a Baseline?

One of these things is not like the other....
What is Your Known Good?

- Baselines
- Asset
- Inventory
- Known traffic
- “Known Good”
Cloud Instances

HOW MANY ARE THERE?
Asset Management

What are your crown jewels?

Where are your crown jewels?

Do you track?

Are you up to date?
Incoming

- Indicators of Compromise IOCs
- Your logs have a story to tell – are you listening?
- Don’t lose sight of what matters most – your own data
- History lessons – logs build context
Sources

- Sensors
- Alerts
- Firewalls
- SIEM
- Email & Spam Filters
- Logging

Automation
So. Many. Alerts
What is your data doing for you?

Data: Care and Feeding of
Enriched ... Just like your favourite breakfast cereal!

- Data Feeds
- Blogs
- Lists
- Alerts
Data Enrichment

Collect Data:
- public
- community
- commercial sources
Data Enrichment

Store Data:
- addresses duplications
- links data
- retains counts of entities
Data Enrichment

Enrich Data:
- DNS
- Whois
- VirusTotal
- lists
Data Enrichment

Relate:
- IP to domain to URL
- IP to ISP to geography
- file hash to malware family
Data Enrichment

- Validate and contextualize against historical details
Enhancement Tactics

- Data Enrichment/Tailoring
- Machine Learning/AI
- Dark Web Monitoring
- OT and Specialized needs
- EUBA/UBA
- Enhanced visibility

Visibility, Content, Context
it's ok to ask for help
Machine Learning /AI

- Predictive threat intel
- Self-learning
- Continuous scanning, sensors
- Harnessing what’s in big data: depth, scale, speed
UBA/EUBA

UBA is a relatively new, but fast growing, form of security detection that alerts on anomalous behavior, rather than traditional signature matches.

User and Entity Behavior Analytics (UEBA) — is a method of detecting malicious activity on a network by correlating information about an organization’s users and entities with anomalous activity.
OT & Specialized Needs

- ICS SCADA environments
- Critical Infrastructure
- More than data loss - destruction of essential systems
- Real-time monitoring of data & connections to see what attackers see
Dark Web Monitoring

- It works differently down here
- Early indicator
- Frequently changing
- Dangerous and difficult to accurately search
The Atlantic Carding Team offers you:
- Credit card information with high validity rate > 95%
- True anonymous communication via PGP-encryption
- Anonymous payment method: Bitcoin
- Escrow-friendly merchants
Multiple feeds are like drinking from a firehose
What is your data doing for you?

Analysis: Threat Correlation
It needs to meet a requirement, to be useful, and respect various forms so that it is open to interpretation and processing.

Robert M. Lee, Principal Dragos Security
Analysis: What Do You Know

- Your own environment
- Your opportunity for harm
- How to use your logs
- Operational vs strategic intelligence
- The phases of an attack i.e., cyber killchain
- Capability: TTP and threat actors
Relevance

- Opportunity: what is the ability for harm to be done. Your people & processes

- Capability: the adversary must have the means to do harm ie PPT

- Intent: This is deliberate. No accident

Per Robert M. Lee
Context

◎ Identify relevant patterns and key data points

◎ Turn data into intelligence

◎ Transform intelligence into knowledge that informs and directs security teams
Figure 5. Integration and complexity issues present remediation challenges for CISOs*

**TECH COMPLEXITY**
Reasons for security technologies being scrapped before or soon after deployment

- The technology was overly complex and too difficult to operate: 77%
- The technology was too expensive to maintain: 41%

**INTEGRATION CHALLENGES ON INTEL**
The problems with current cyber threat intelligence

- Threat intelligence activities/processes are difficult to manage: 64%
- Does not integrate easily with various security technologies: 59%
- Threat intelligence activities/processes are very complex: 56%

**MISALIGNED SYSTEMS**
Areas of potential cybersecurity risk within the IT environment today

- Organizational misalignment and complexity: 33%
- Lack of system connectivity/visibility: 30%

*Multiple industries, with financial services forming largest segment of the respondent base at 22%.

Patterns

Comparison of "SWIFT" malware with North Korea's malware

South Korea's Media Hack (Jun 2013) by North Korea

Sony Pictures Hack (Nov 2014) by North Korea

Vietnam Bank Hack (Dec 2015) by ?

Bangladesh Bank Hack (Feb 2016) by ?

Connect
The
Dots

Similar with Wipe-out function

From https://twitter.com/issuemakerslab
(Simon & Taylor)
Anomalies

Monitor everything
Logs, network traffic, user activity

Correlate intelligently
Connect the dots of disparate activity

Detect anomalies
Unusual yet hidden behavior

Prioritize for action
Attack high-priority incidents

Correlation

The “Secret Sauce” to pull it all together
What is your data doing for you?

Target Takes Aim: Flip that table
The Pyramid of Pain

The Pyramid measures the potential usefulness of your intel

Aim high - The harder you make it for your adversaries

The Pyramid of Pain, originally developed by David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
The Diamond Model of Intrusion Analysis

### Pivot and Cyber Kill Chain

<table>
<thead>
<tr>
<th>Stage</th>
<th>Attack Graph</th>
<th>Activity Thread</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weaponization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action on Objectives</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Victim₁

DGA: Domain Generation Algorithms New Threats

- A program providing malware with new domains on the fly
- C+C servers for botnets and ransomware. Block these and break the link between victim and attacker
- Increasing tactic based on older technique abusing DNS load balancing
What is your data doing for you?

Conclusion & Recap
Recap

- Threat Intel is …
- Care & Feeding of your data
- New & Improved
- Playtime: Loops & Chains
Thank You!

Any questions?

You can find me at:
@3ncr1pt3d
https://whitehatcheryl.wordpress.com