



# **Threat Intel for All: There's More to Your Data than Meets the Eye**

By @3ncr1pted  
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



A decorative background featuring a network of nodes and lines, resembling a molecular structure or a complex web, in a light gray color.

# 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

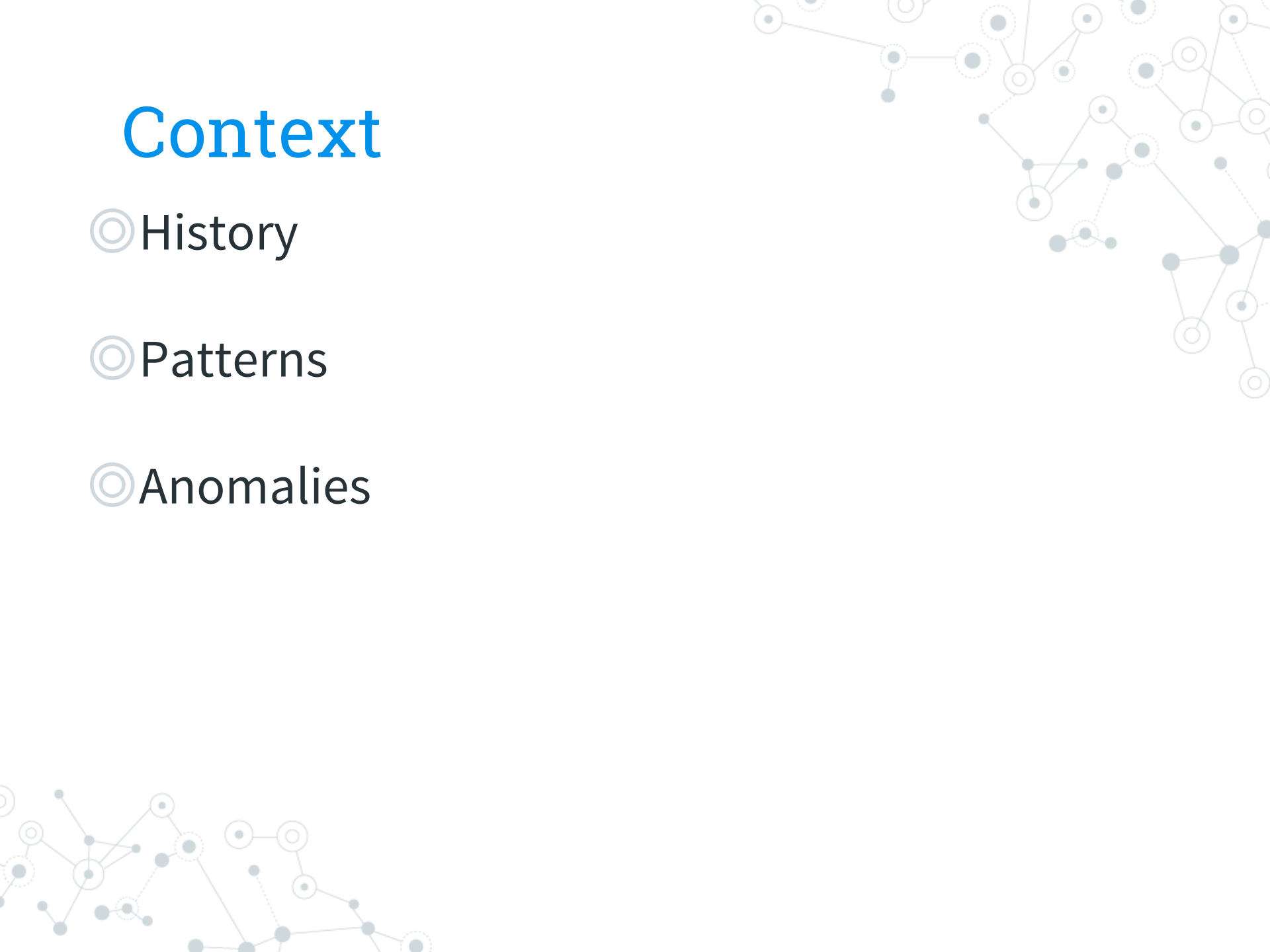
- ◎ “Finished Intelligence” – data made to measure for you
- ◎ Go for good, not great. Get it up and running
- ◎ Opportunity, Capability, Intent – make it relevant
- ◎ Threat Intel Fusion points
- ◎ Objectives: become proactive

# Context

◎ History

◎ Patterns

◎ Anomalies



# Relevance

Yes, but what does this mean to ***you***?



“

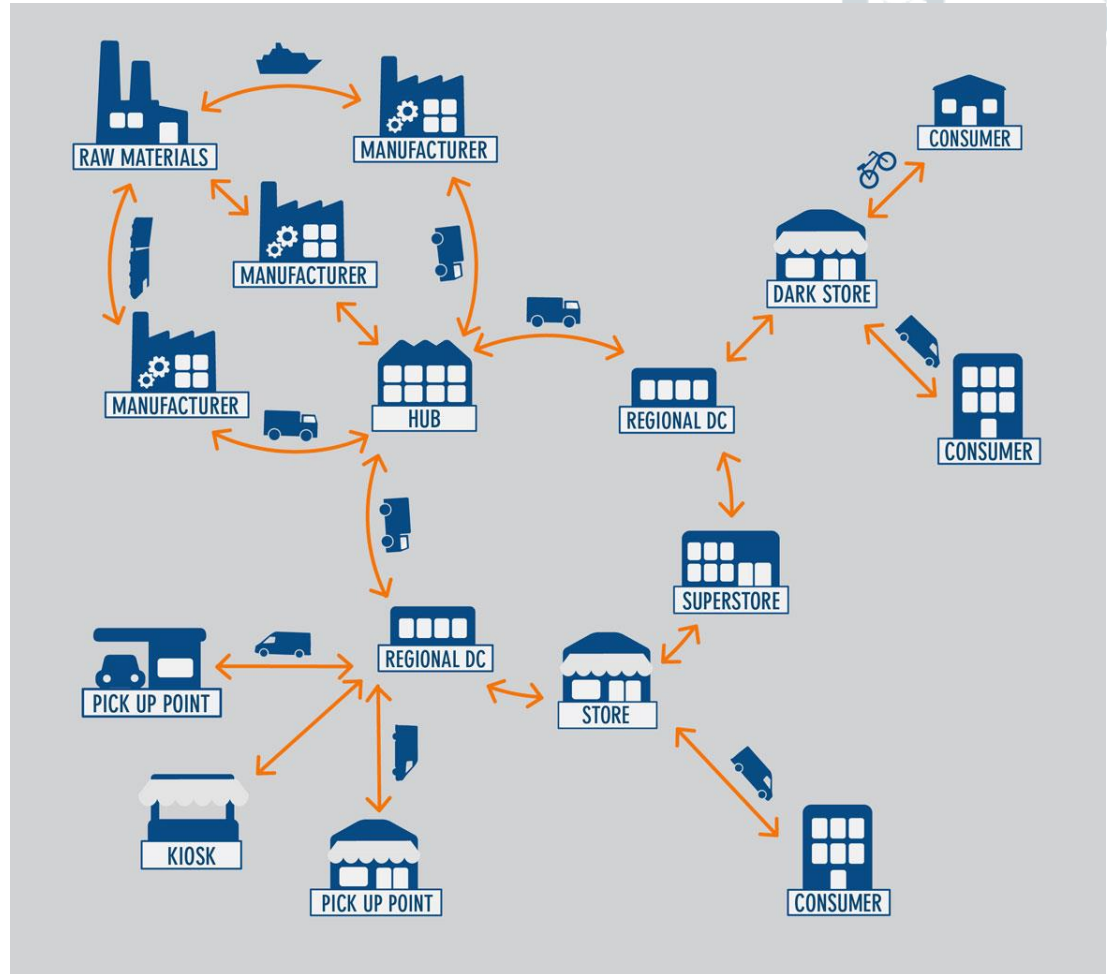
*There is no more relevant threat intelligence than what is actually occurring within your organization*

*Rick Holland, Forrester Research*

# Objective

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

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**

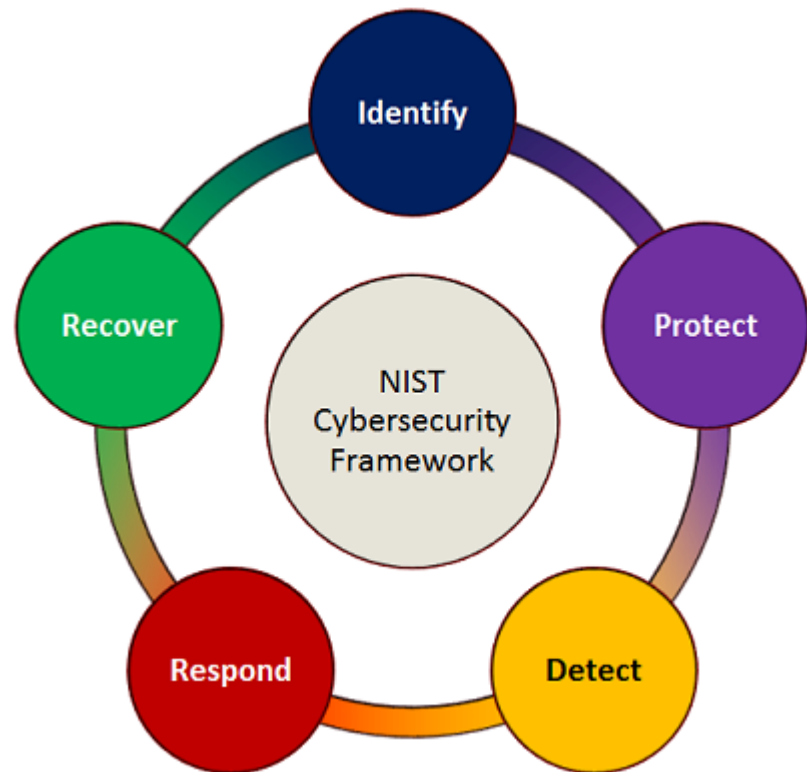


# Why a Baseline?



# What is Your Known Good?

- ◎ Baselines
- ◎ Asset Inventory
- ◎ Known traffic
- ◎ “Known Good”



# Cloud Instances



# 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

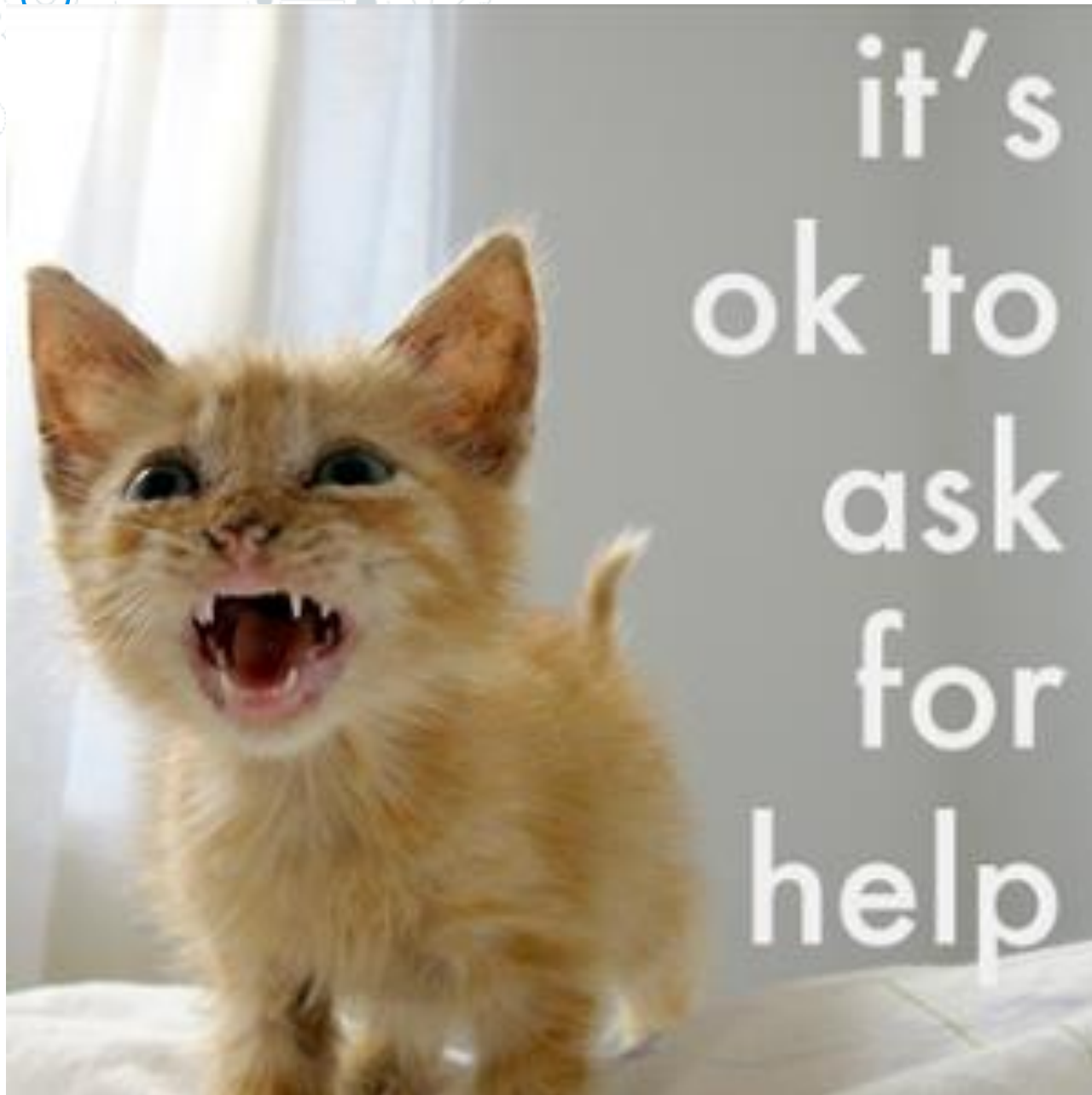
- ◎ Validate and contextualize against historical details



# Enhancement Tactics

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

*Visibility, Content, Context*





# 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







# ATLANTIC CARDING

[USA](#)
[CANADA](#)
[EUROPE](#)





[Home](#)
[Products](#)
[Contact Us](#)
[Information](#)

**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

Whonix-Workstation [Running] - Oracle VM VirtualBox

[File](#)
[Machine](#)
[View](#)
[Input](#)
[Devices](#)
[Help](#)

[OUTLAW Market - Tor Browser](#)

[Whonix Welcome P...](#)
[torch tor search ...](#)
[How to access ...](#)
[SBC - Grams](#)
[Search results f...](#)
[Search results potash](#)


[outfor6jwcztwbpd.onion/index.php?step=choose&search](#)

1 BTC = 741 USD
DM
Listings
Messages
Profile
Orders
Account

☒ regular offers
☒ DDs
☒ auctions
☒ FE
Set
All offers shown ==click for domestic only==
100 items/page

Sorting: [alphabet](#) | [cheapest](#) | [newest](#) | [bestseller](#) | [discounted](#) | [fastest delivery time](#) | [most rel](#)

**Depanage (4.364/5-4/5) uses OUTLAW escrow**  
**Depanage presents:**  
3g S-isomer Ketamine




Quality: highest / purest  
Für die ersten 20 Bestellungen: 10 % Rabatt! In den Volkssagen der Hindus verkörpert Durga Marta als Gottesmutter Reinheit und Stärke. Sie trägt das Schwert der Wahrheit, zerstört Dämonen, überwindet Schranken der Ignoranz und führt die Menschen zur Erleuchtung. Durga Marta wird deinen inneren

price: 58.96 USD

 BDA

**GreenSupreme (5/5-5/5) uses MULTISIG**  
Discount (RY4FY5)  
**GreenSupreme presents:**  
5g Durga Mata III \*\*\*The Mother Goddess\*\*\*



Quality: highest / purest  
Für die ersten 20 Bestellungen: 10 % Rabatt! In den Volkssagen der Hindus verkörpert Durga Marta als Gottesmutter Reinheit und Stärke. Sie trägt das Schwert der Wahrheit, zerstört Dämonen, überwindet Schranken der Ignoranz und führt die Menschen zur Erleuchtung. Durga Marta wird deinen inneren

price: 56.28 USD 50.65 USD

**GreenSupreme (5/5-5/5) uses OUTLAW escrow**  
**GREEN USA presents:**  
7g Power Plant Medical Grade Sativa 21.4% THC - .1% CBD

Quality: highest / purest  
As always our shipments arrive vacuum sealed with zero smell. Power Plant

**GreenSupreme (5/5-5/5) uses OUTLAW escrow**  
**GREEN USA presents:**  
7g Private Reserve Medic...

Quality: high  
As always our sealed with n

**Weed (556)**  
**Medication (422)**  
**Hash (262)**  
**Cocaine (129)**  
**MDMA (124)**  
**Amphetamines (107)**  
**XTC-pills (102)**

“

*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 ie cyber killchain
  - ◎ Capability: TTP and threat actors
- 

# Relevance

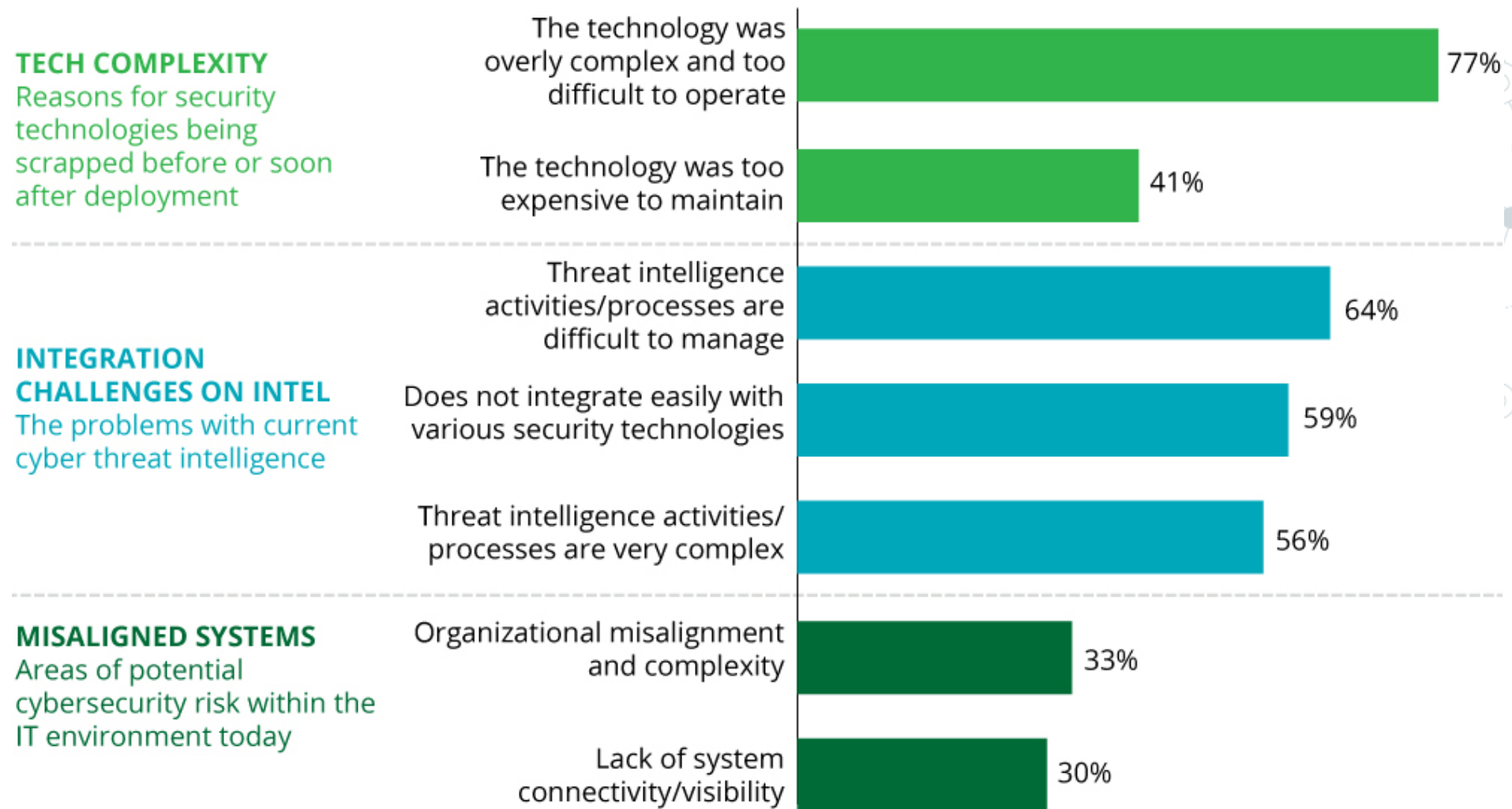
- ◎ Opportunity: what is the ability for harm to be done. Your people & processes
- ◎ Capability: the adversary must have the means to do harm ie PPT
- ◎ Intent: This is deliberate. No accident

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\***



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

Sources: Lockheed Martin and Ponemon Institute, *Intelligence-driven cyber defense*, February 2015; Lockheed Martin and Ponemon Institute, *Risk and innovation in cybersecurity investments*, April 2015.

# Patterns

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

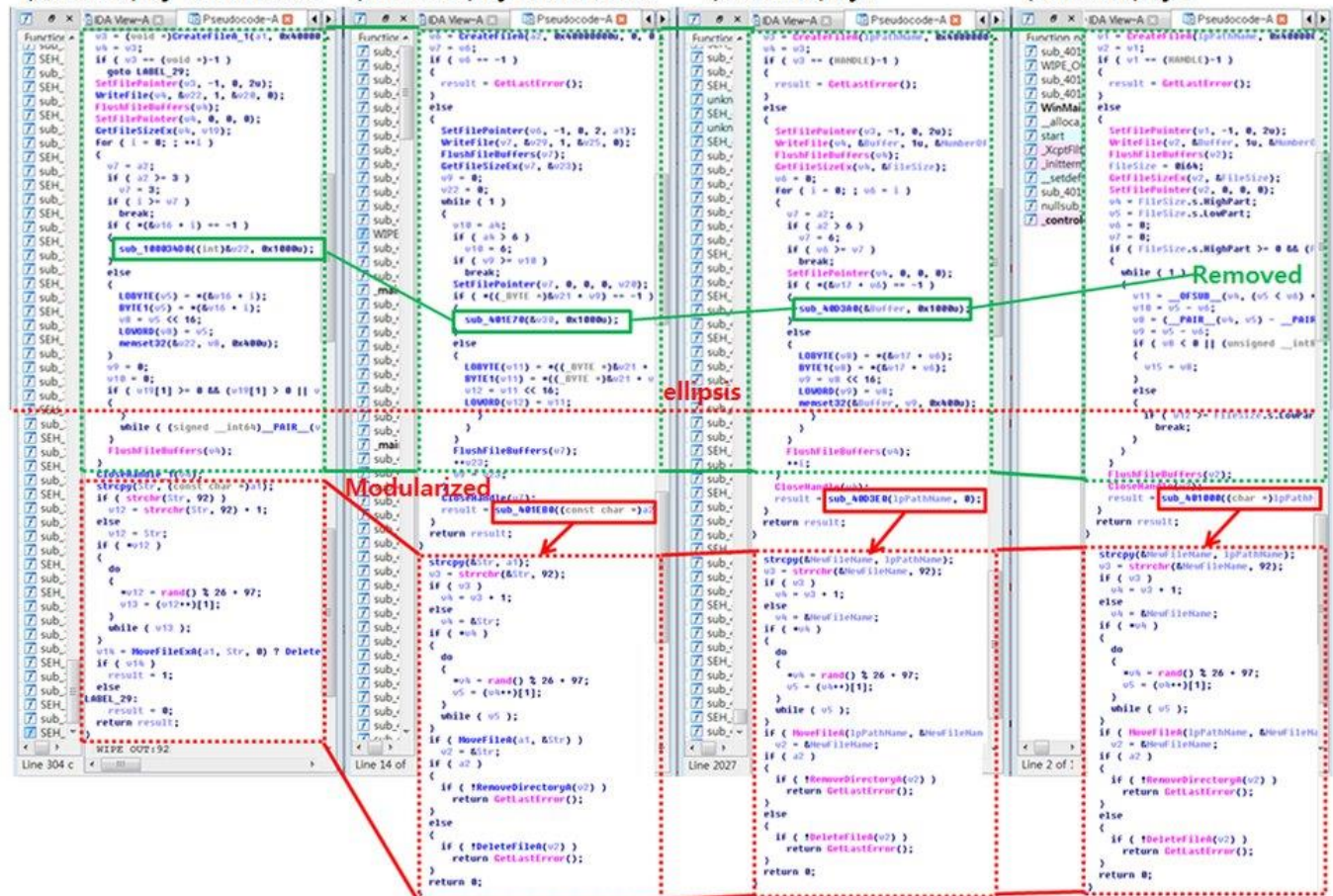
South Korea's Media Hack  
(Jun 2013) by North Korea

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)



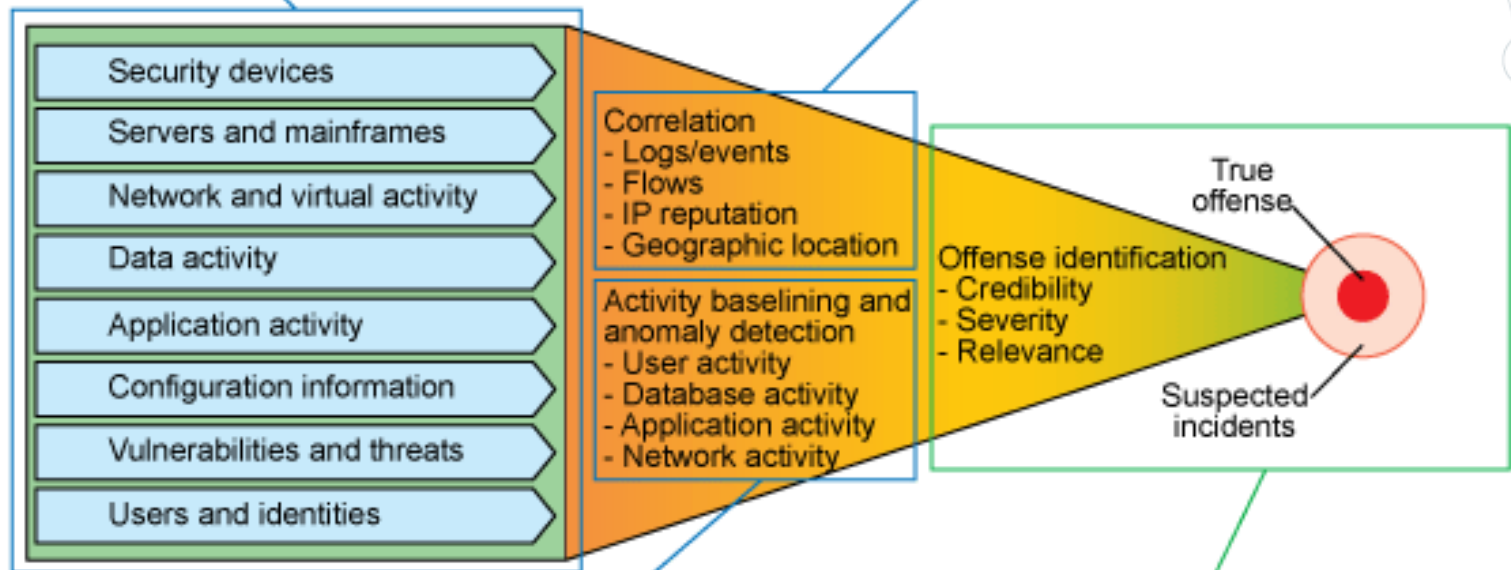
# Anomalies

## Monitor everything

*Logs, network traffic, user activity*

## Correlate intelligently

*Connect the dots of disparate activity*



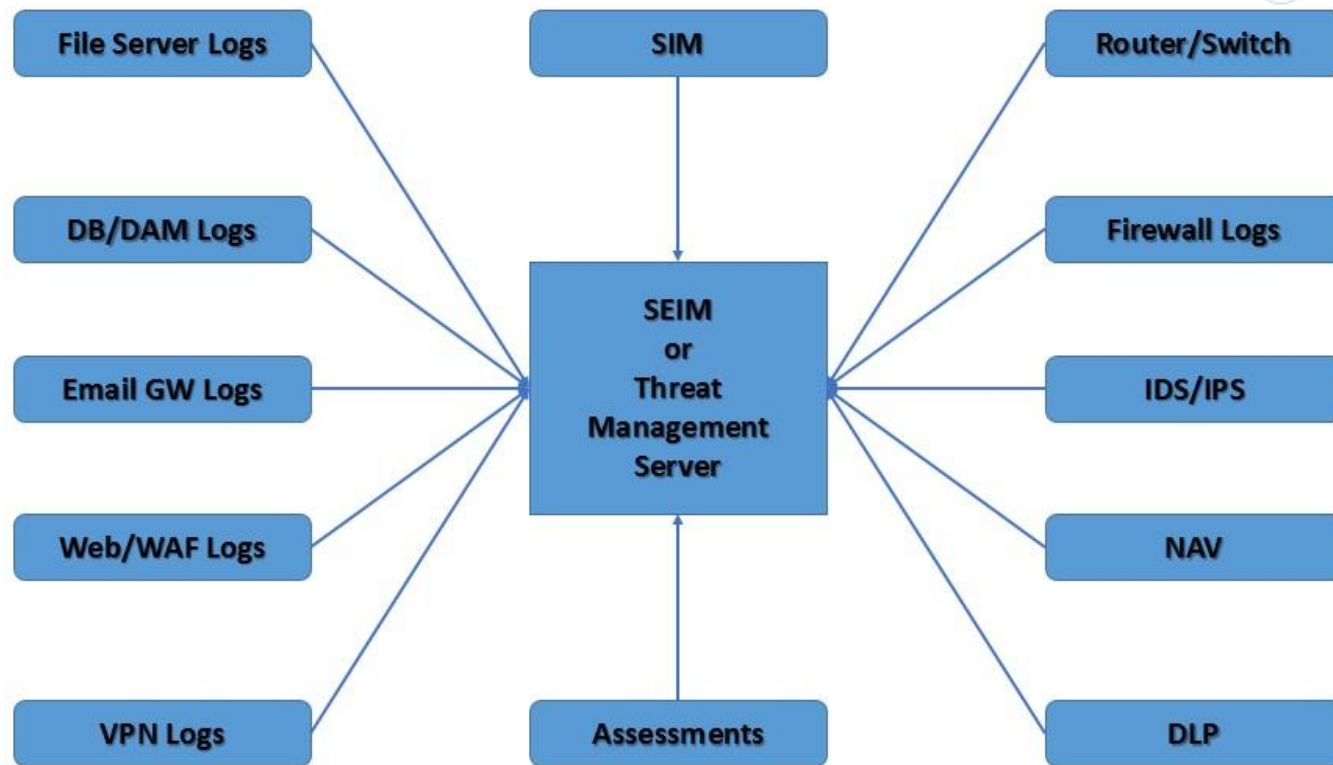
## Detect anomalies

*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?*

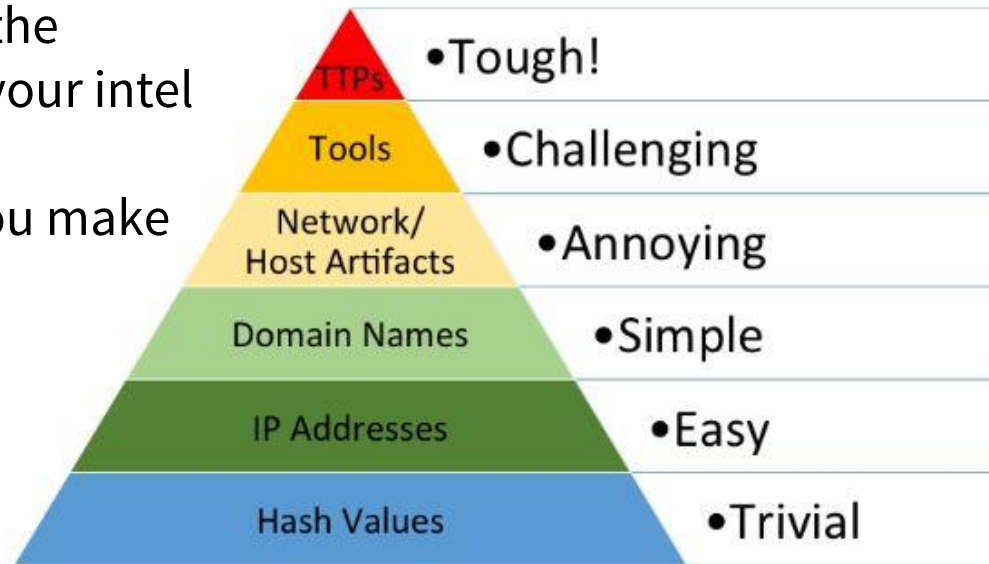
**Target Takes Aim: Flip that  
table**



# The Pyramid of Pain

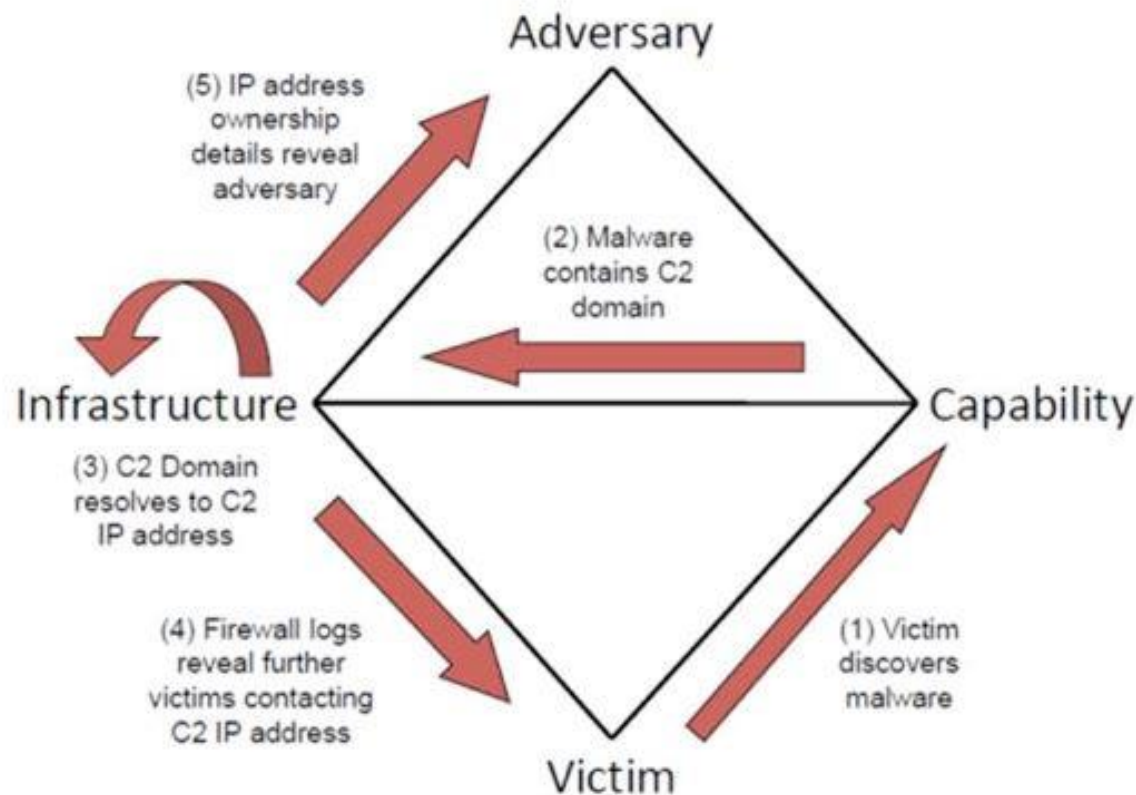
The Pyramid measures the potential usefulness of your intel

Aim high - The harder you make it for your adversaries

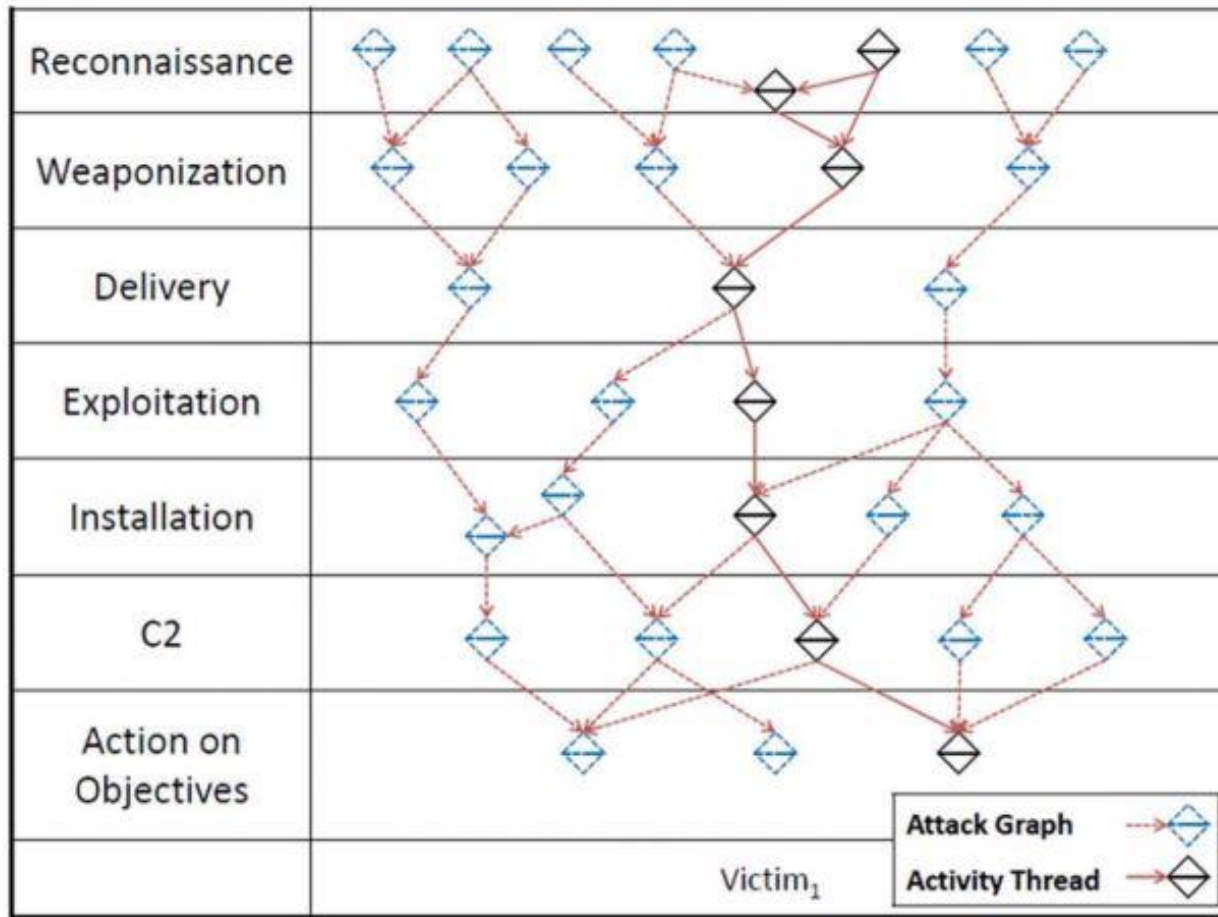


The Pyramid of Pain, originally developed by David Bianco: <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

# The Diamond Model of Intrusion Analysis



# Pivot and Cyber Kill Chain



# 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

A decorative network diagram at the top of the slide, featuring a series of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some solid and some dashed, connected by thin lines. A central node is highlighted with a larger, dashed circle around it, containing a blue double quote symbol.

“

*What is your data doing for you?*

## **Conclusion & Recap**

A decorative background featuring a network diagram with nodes and connecting lines, primarily located in the top-left and bottom-right corners. The nodes are represented by circles of varying sizes, some with concentric rings, and the lines are thin and grey.

# Recap

- Threat Intel is ...
- Care & Feeding of your data
- New & Improved
- Analysis: Context. Patterns. Anomalies. Correlation
- Playtime: Loops & Chains



# Thank You!

## Any questions?

You can find me at:

@3ncr1pt3d

<https://whitehatcheryl.wordpress.com>

