FREDDY DEZEURE

Intel Driven Detection / Prevention

October 2017

About Me

- Consultancy
  - Independent Strategic Advisor
  - Trainer C-Suite/Board
  - Board Member EclecticIQ
  - Advisory Board Member SpyCloud, Intel471, Phantom Cyber
- Thirty years at the European Commission
  - Head of CERT-EU, protecting 100.000 users in 60 organizations
  - COO, CRO at the Joint Research Centre (3000 scientists)
  - Internal and external audit
- Five years as CIO in private industry

Agenda

- General Context
- Threat Intelligence
- Maturity Gap and Opportunities
- One more thing

(Not)Petya June 2017

PRESS ANY KEY!

- Initial distribution via MeDoc
- Disruptive intent in UA
- Disruption worldwide
- Massive economic impact

Impact

Maersk/APM

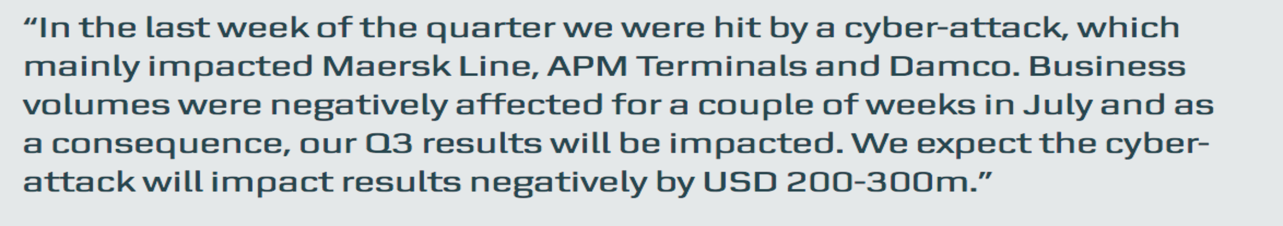
- 17 container terminals disrupted for days
- Loading and unloading impossible because of uncertainty of the shipments
- Delays down the logistic chain
- Perishable goods lost?

FedEx/TNT

- Parcels with next day delivery commitment were not delivered after a month
- Customers had to resubmit documents for parcels already in transit
- Lost parcels?

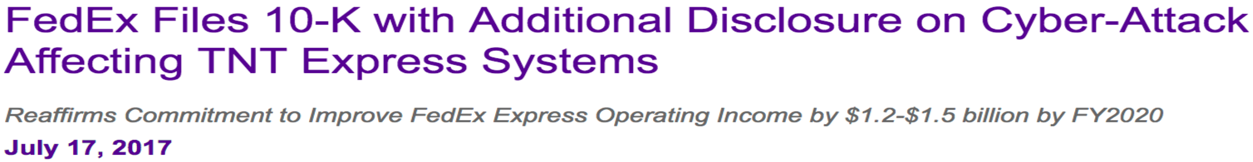
Impact

Maersk/APM



"In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by USD 200-300m."

FedEx/TNT



FedEx Files 10-K with Additional Disclosure on Cyber-Attack Affecting TNT Express Systems

Reaffirms Commitment to Improve FedEx Express Operating Income by $1.2-$1.5 billion by FY2020

July 17, 2017

"It is reasonably possible that TNT will be unable to fully restore all of the affected systems and recover all of the critical business data..."

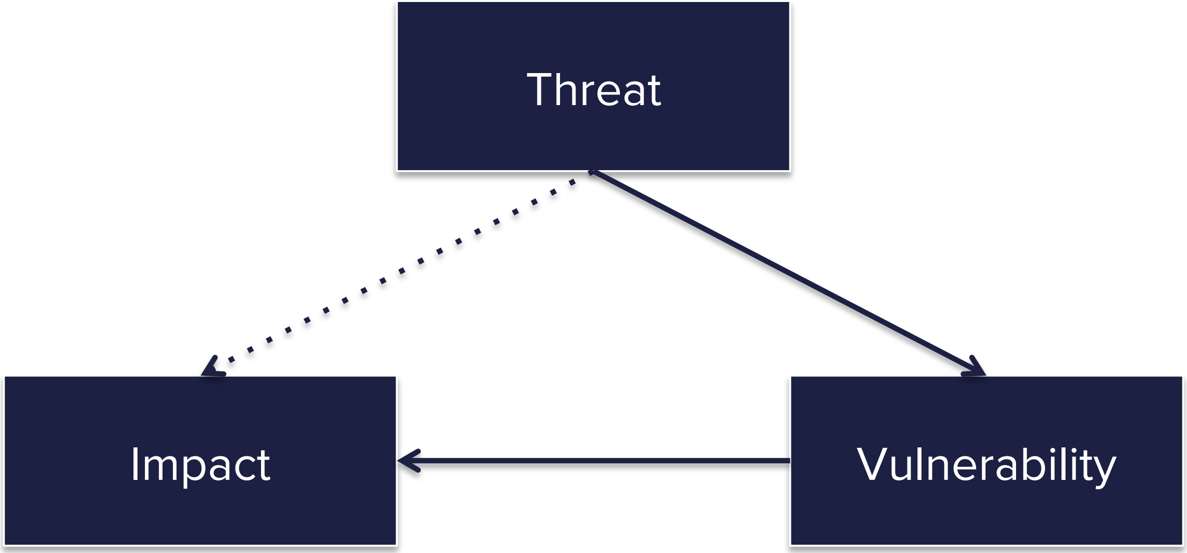
"We are still evaluating the financial impact of the attack, but it is likely that it will be material"

General Context

- Dependent
  - Service delivery requires connectedness
  - Distributed systems (factories, cars, health…)
  - Everything and everybody exposed
- Vulnerable
  - Broad attack surface
  - Inherently fragile systems
  - Often unpatchable
- Determined Adversaries
  - Industrialisation of exploit development
  - Leakage and proliferation of sophisticated techniques

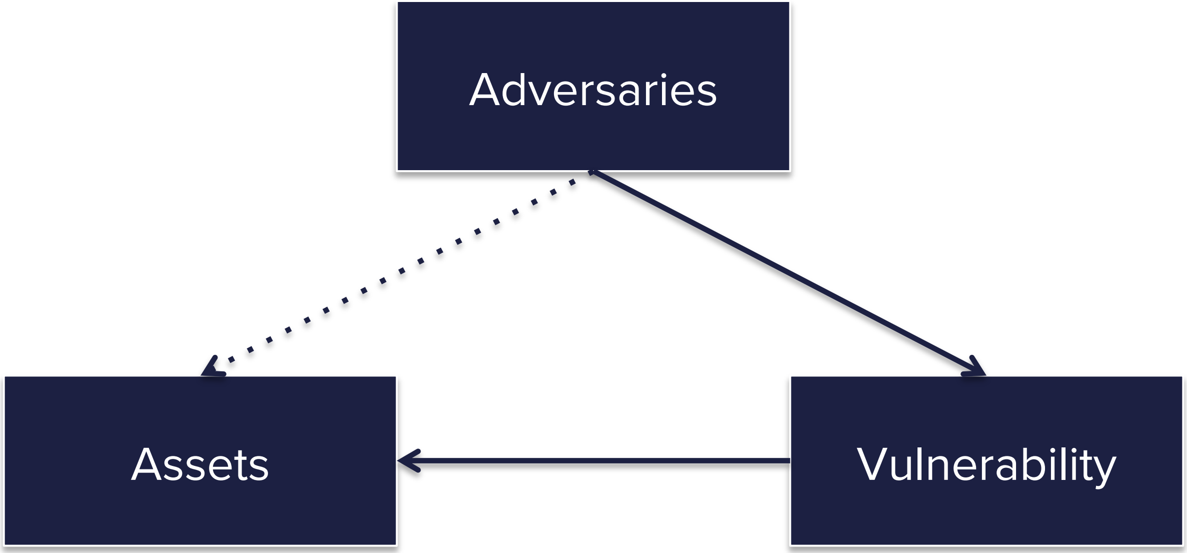
Risk

Threat x Vulnerability x Impact



Risk

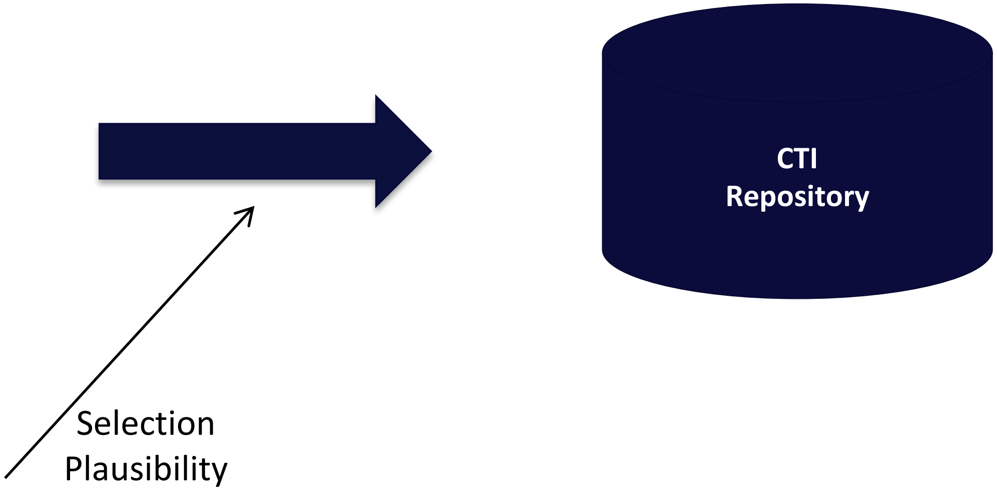
Threat x Vulnerability x Impact



Observe

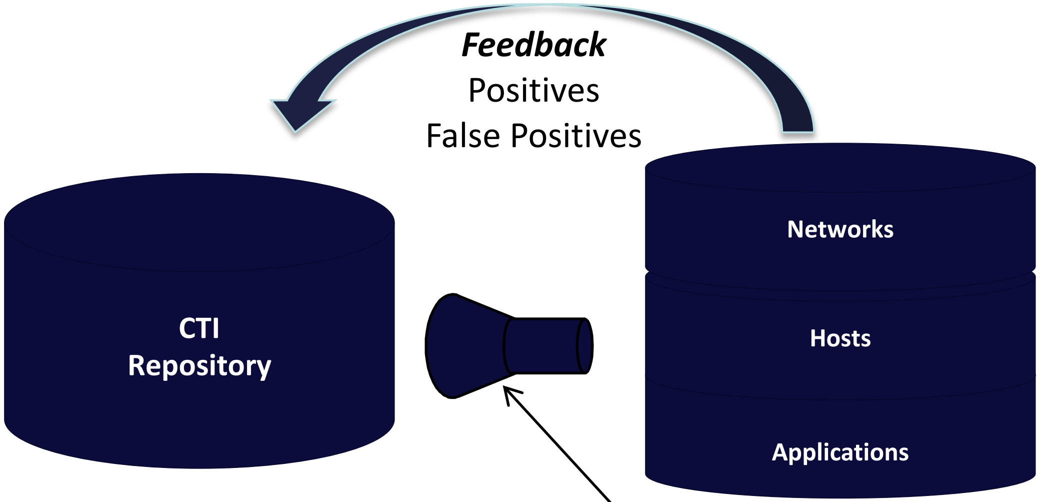
Key Questions

- Who?
- What?
- Why?
- How?
- When?
- Does it matter to us?



Selection
Plausibility
Enrichment
Contextualization

Operationalise



Feedback

Positives

False Positives

Correlation

Taxonomy

Selection

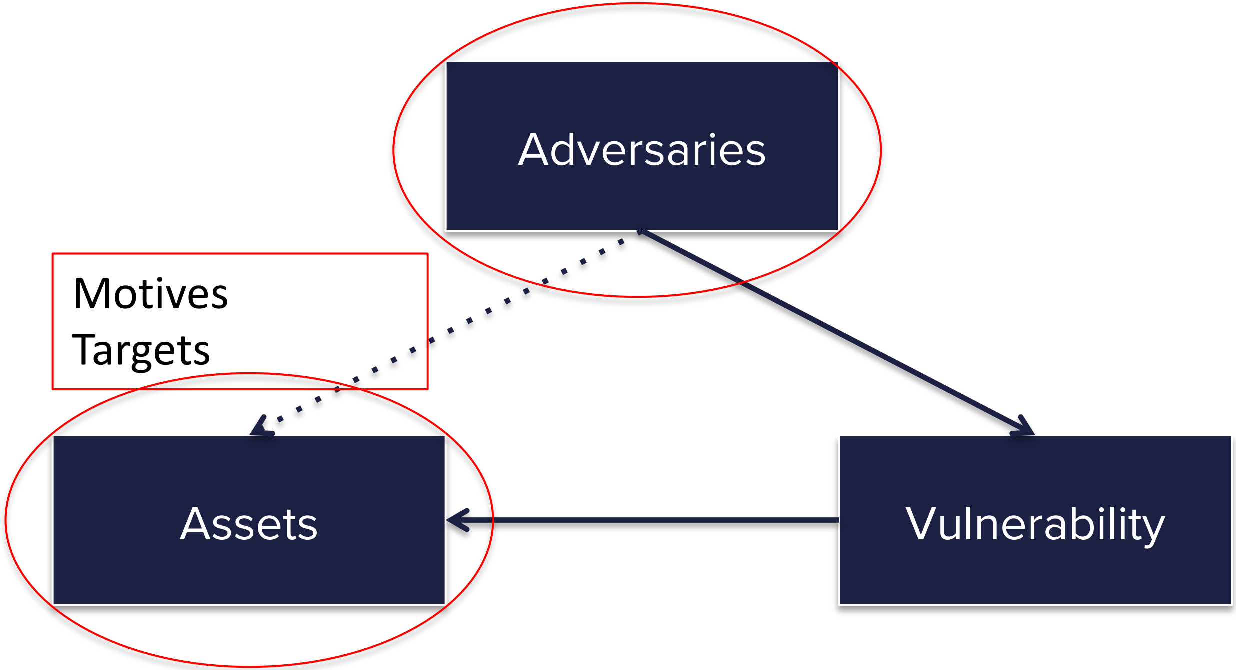
Formatting

Routing

Course of Action

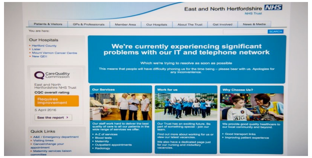
Threat Intelligence

Threat x Vulnerability x Impact



Motives/Targets

- Financial Gain
  - Targeted ransomware, blackmailing
  - Diverting financial transactions
  - Benefitting from inside information
  - Market manipulation



You are here:

Our Hospitals
- Hertford County
- Lister
- Mount Vernon Cancer Centre
- New QEII

Care Quality Commission

East and North Hertfordshire NHS Trust

CQC overall rating

Requires improvement

5 April 2016

See the report ›

Quick Links
- A&E / Emergency department
- Visiting times
- Cancel/change your appointment
- Maternity services liaison committee

We're currently experiencing significant problems with our IT and telephone network

Which we're trying to resolve as soon as possible

This means that people will have difficulty phoning us for the time being – please bear with us. Apologies for any inconvenience.

Our Services

Our staff work hard to deliver the best quality of care to all our patients in the wide range of services we offer.
- A-Z of services
- Blood tests
- Maternity
- Outpatient appointments
- Radiology

Work for us

Our Trust has an exciting future. Be part of something special - join our team.

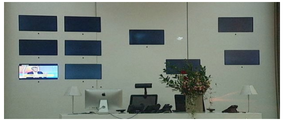
Find out more about working for us or view our latest vacancies.

We also have a dedicated page just for our nursing and midwifery vacancies.

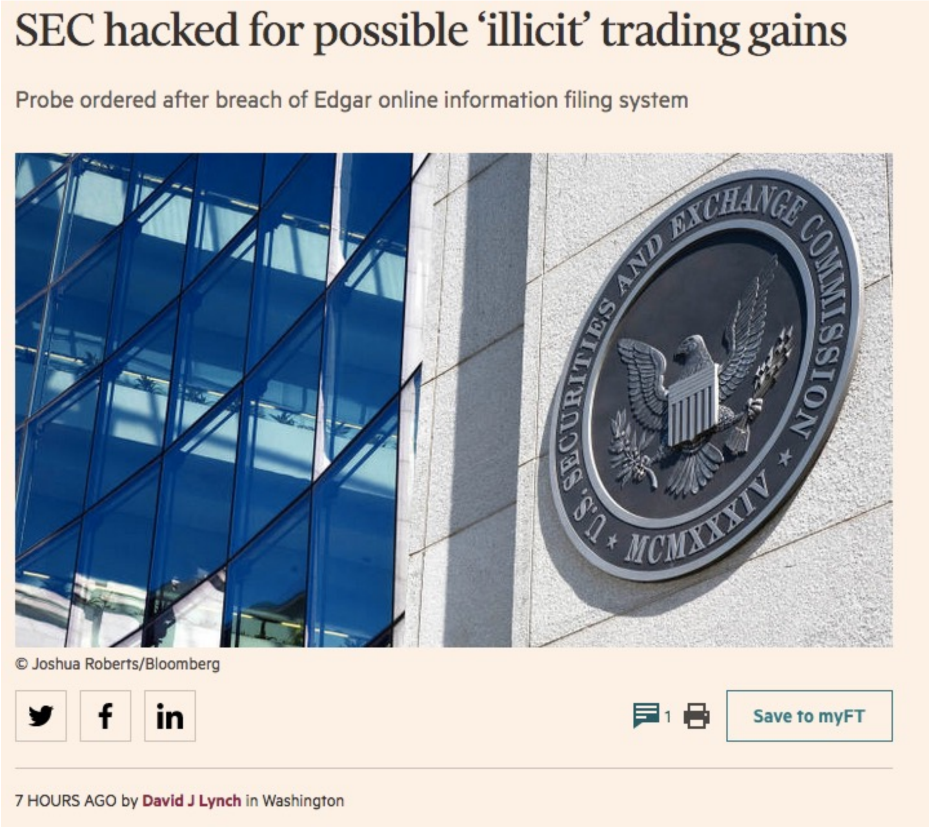
Why Choose Us?

We provide good quality healthcare to our local community and beyond.
- Good transport links
- Improving patient experience

- Improve Position
  - Compete (IPR, business information)
  - Oppress political adversaries, manipulate press, opinion
- Disrupt
  - Strategic
  - (Terrorism)



Inside Information



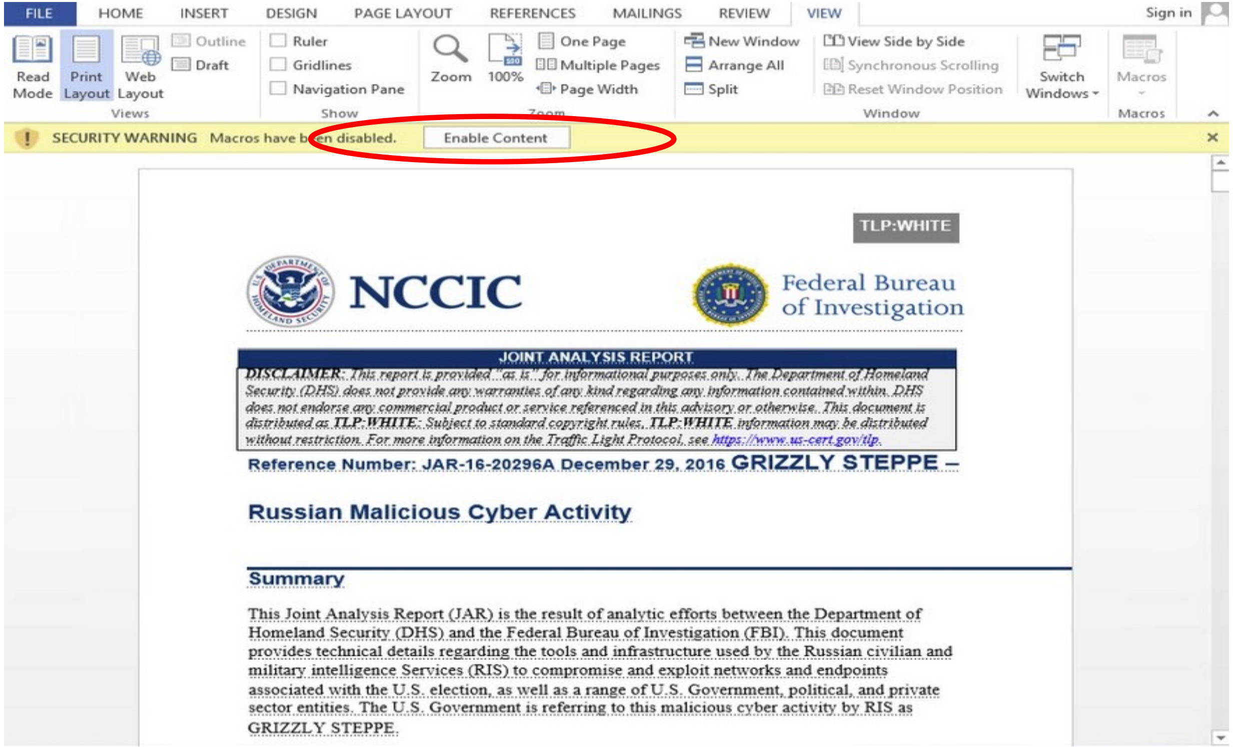
SEC hacked for possible ‘illicit’ trading gains

Probe ordered after breach of Edgar online information filing system

© Joshua Roberts/Bloomberg

7 HOURS AGO by David J Lynch in Washington

Targeting Us



TLP:WHITE

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE****: Subject to standard copyright rules.* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296A December 29, 2016 GRIZZLY STEPPE –

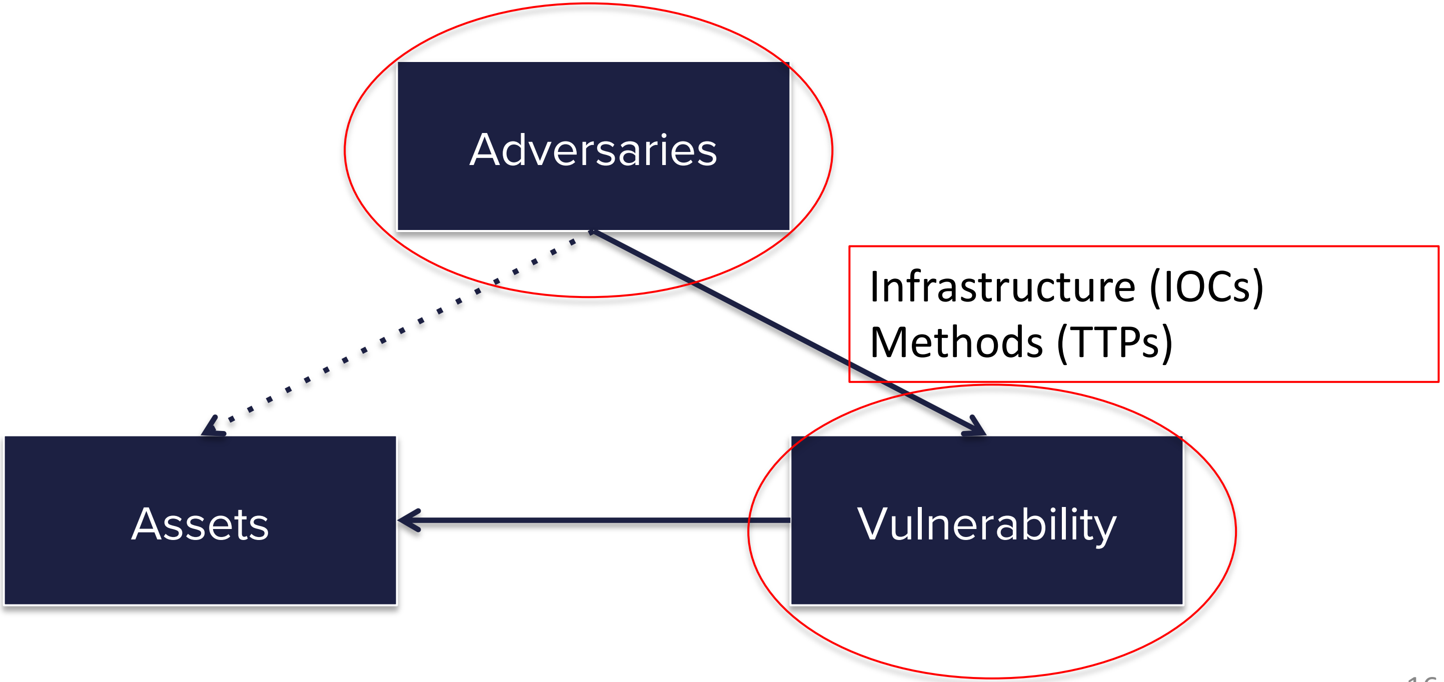
Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Threat Intelligence

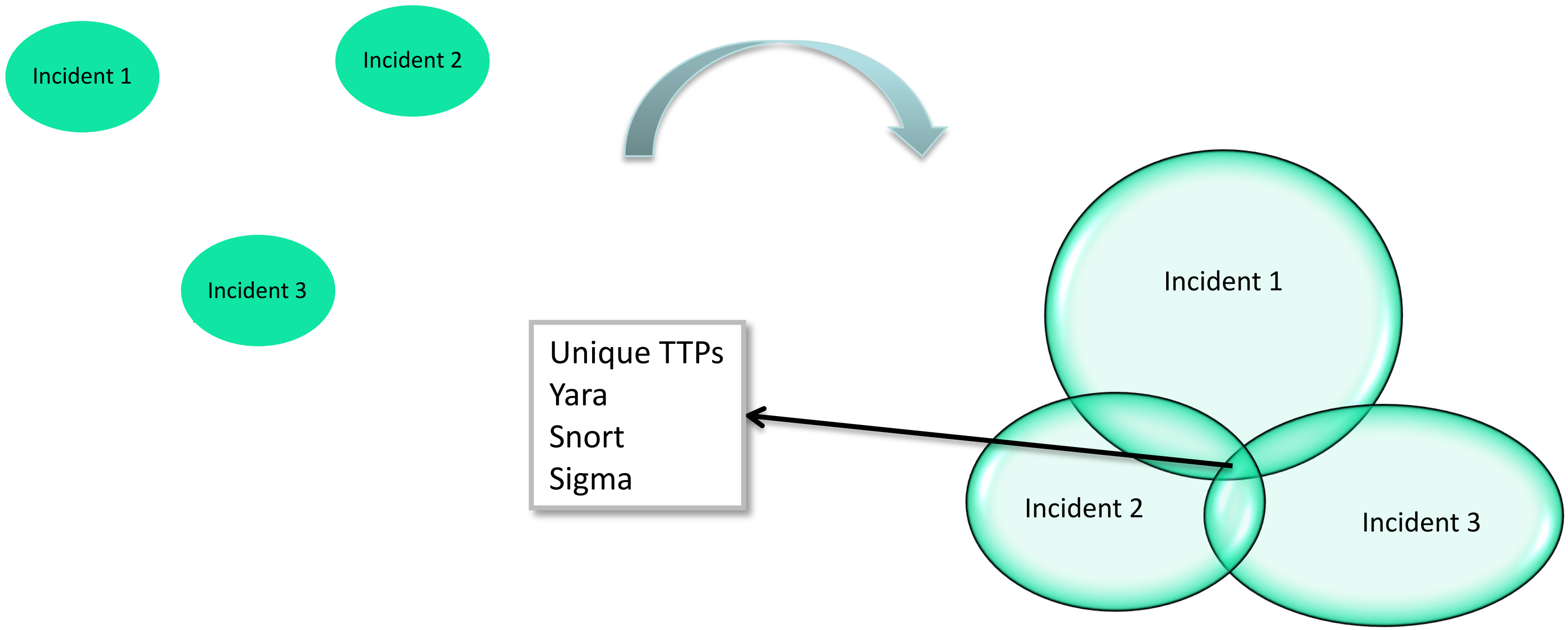
Threat x Vulnerability x Impact



IOC Challenges

- Detection becomes more and more difficult
- Very short-lived
  - Domains: Very high number of domains, freshly registered
  - IPs: Changing: active, parking, legit
  - MD5: Victim-specific malware
  - Email metadata: changing on a daily basis
- Blending in with the user
  - User agent
  - Proxy credentials
  - Timing / batch processing
  - Legitimate domains as C&C

TTPs are more stable



Incident 1

Incident 2

Incident 3

Unique TTPs
Yara
Snort
Sigma

Incident 1

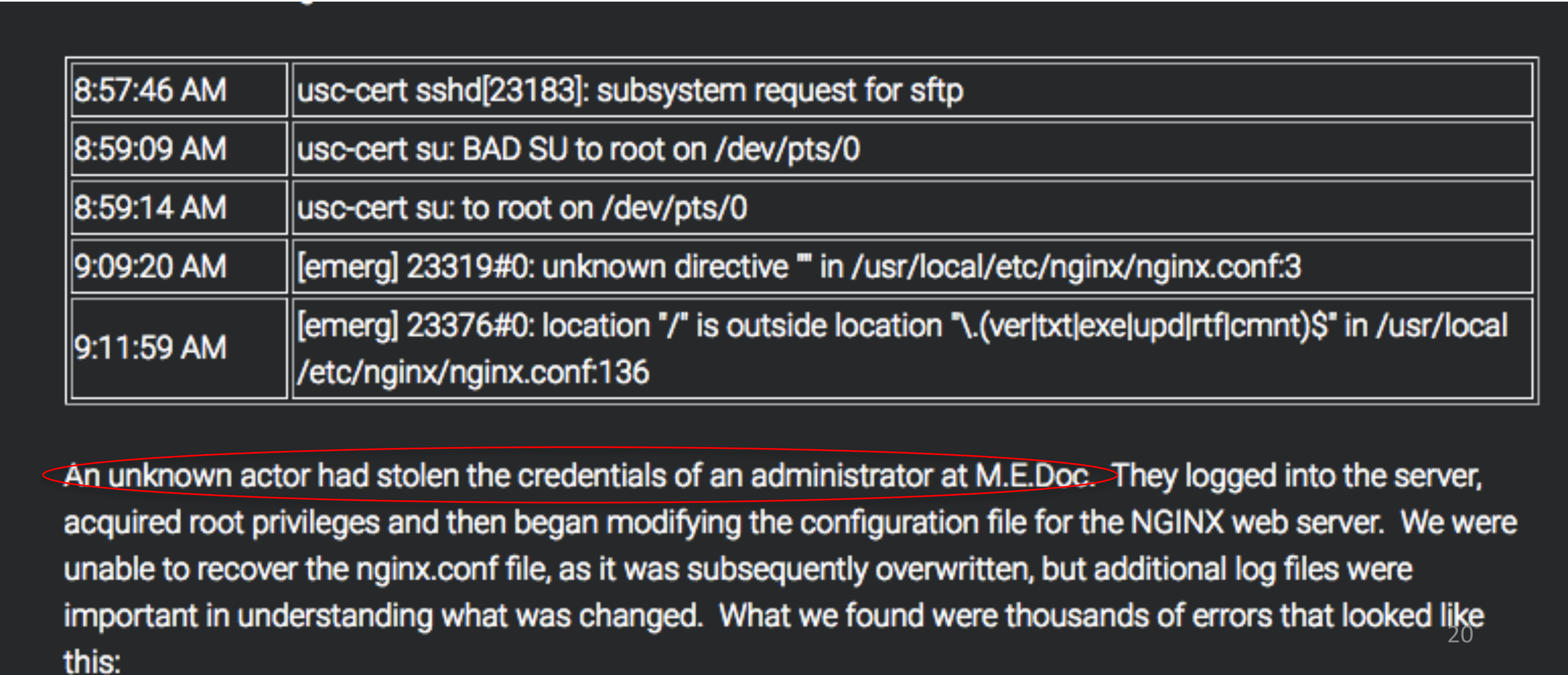
Incident 2

Incident 3

Stealthier

- Prevention becomes more and more difficult
- Spear phishing emails bypassing protective layers
  - Mimicking trusted parties
  - Unpatched vulnerabilities
  - Non-active or low-active content (JavaScript, Macros)
  - Encrypted, password protected, attachments
- Using legitimate OS components (PowerShell, WMI)
- Using legitimate credentials

(Not)Petya

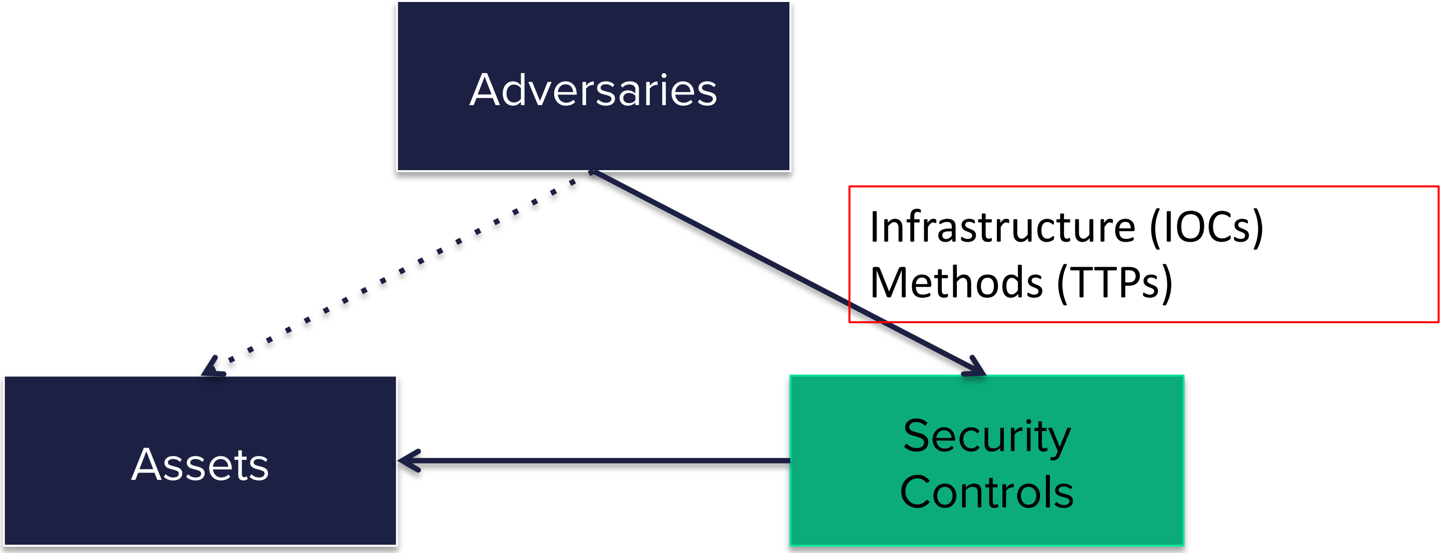


<table>
<tr><td>8:57:46 AM</td><td>usc-cert sshd[23183]: subsystem request for sftp</td></tr>
<tr><td>8:59:09 AM</td><td>usc-cert su: BAD SU to root on /dev/pts/0</td></tr>
<tr><td>8:59:14 AM</td><td>usc-cert su: to root on /dev/pts/0</td></tr>
<tr><td>9:09:20 AM</td><td>[emerg] 23319#0: unknown directive """ in /usr/local/etc/nginx/nginx.conf:3</td></tr>
<tr><td>9:11:59 AM</td><td>[emerg] 23376#0: location "/" is outside location "\.(ver|txt|exe|upd|rtf|cmnt)$" in /usr/local /etc/nginx/nginx.conf:136</td></tr>
</table>

An unknown actor had stolen the credentials of an administrator at M.E.Doc. They logged into the server, acquired root privileges and then began modifying the configuration file for the NGINX web server. We were unable to recover the nginx.conf file, as it was subsequently overwritten, but additional log files were important in understanding what was changed. What we found were thousands of errors that looked like this:

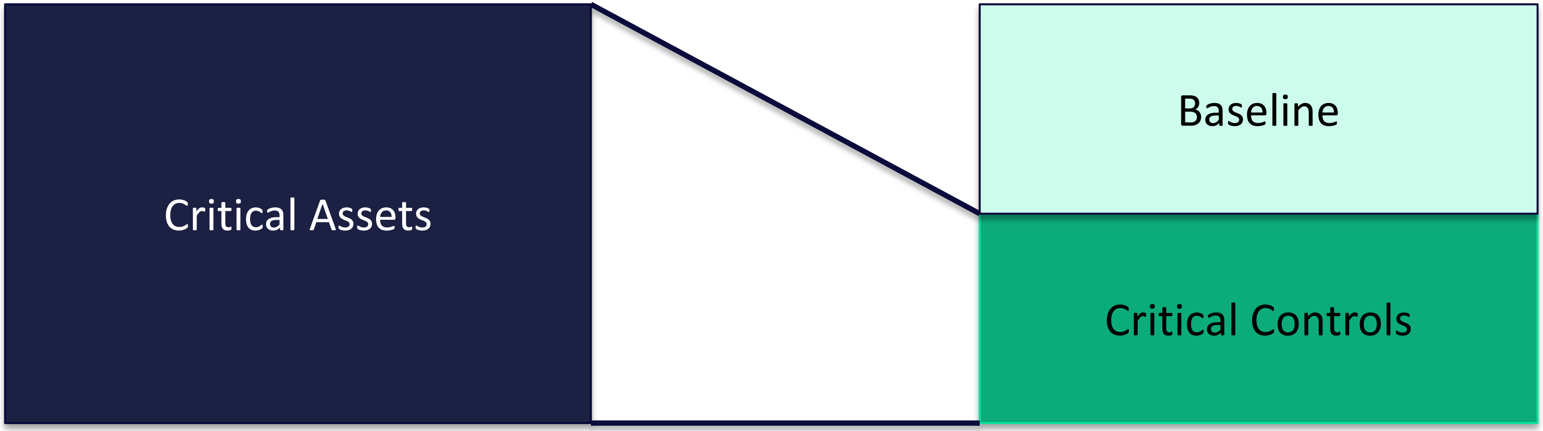
Prevention

Threat x Vulnerability x Impact



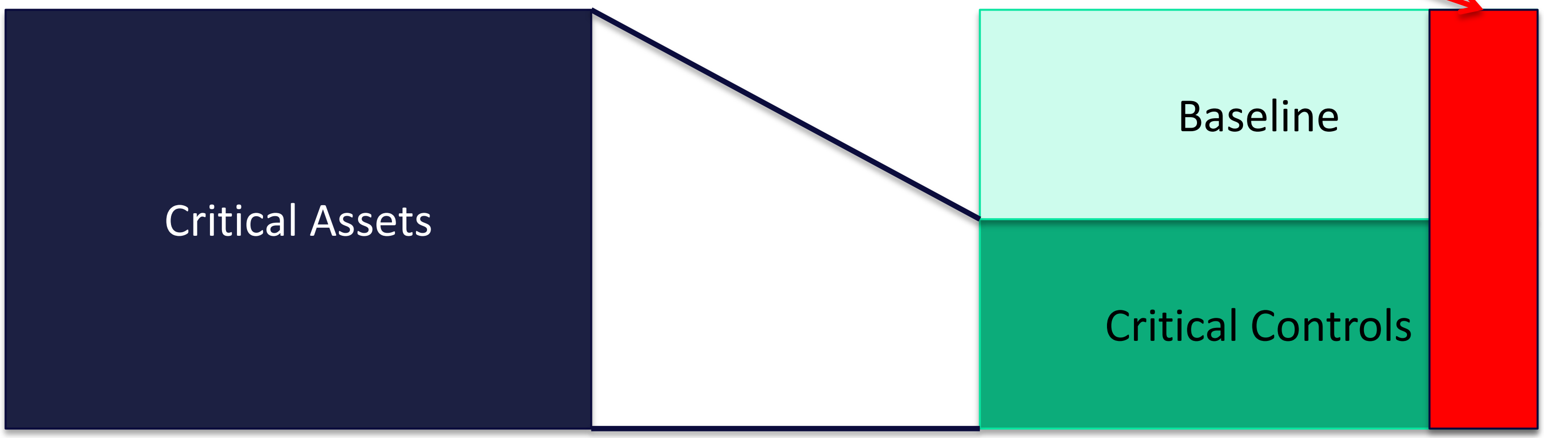
Infrastructure (IOCs)
Methods (TTPs)

Prevention



Check Against New TTPs

New vulnerabilities
New methods (TTPs)

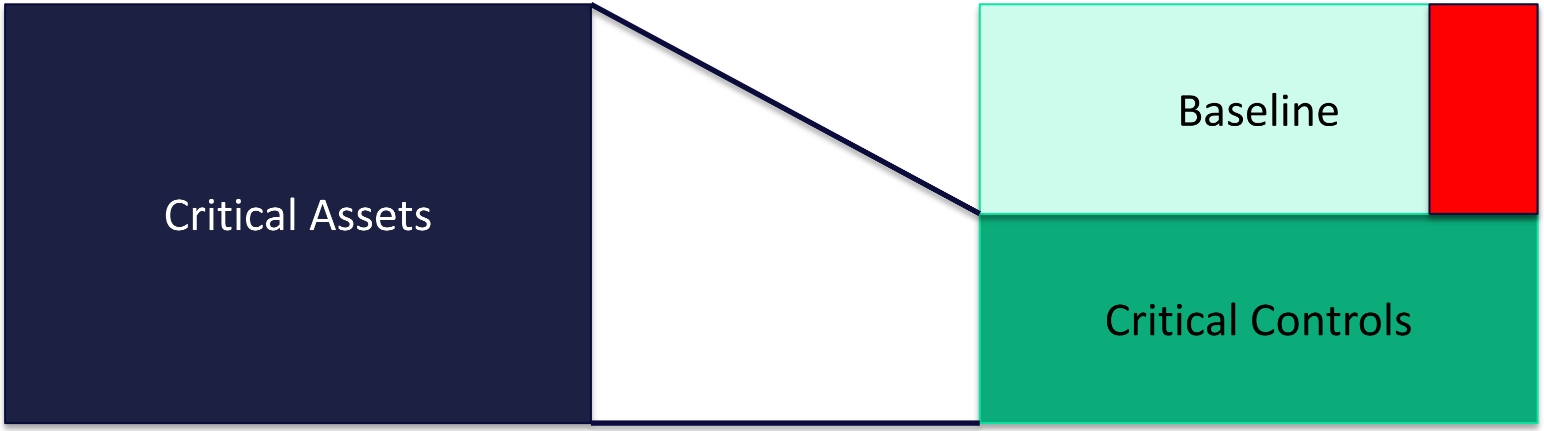


Critical Assets

Baseline

Critical Controls

Adapt

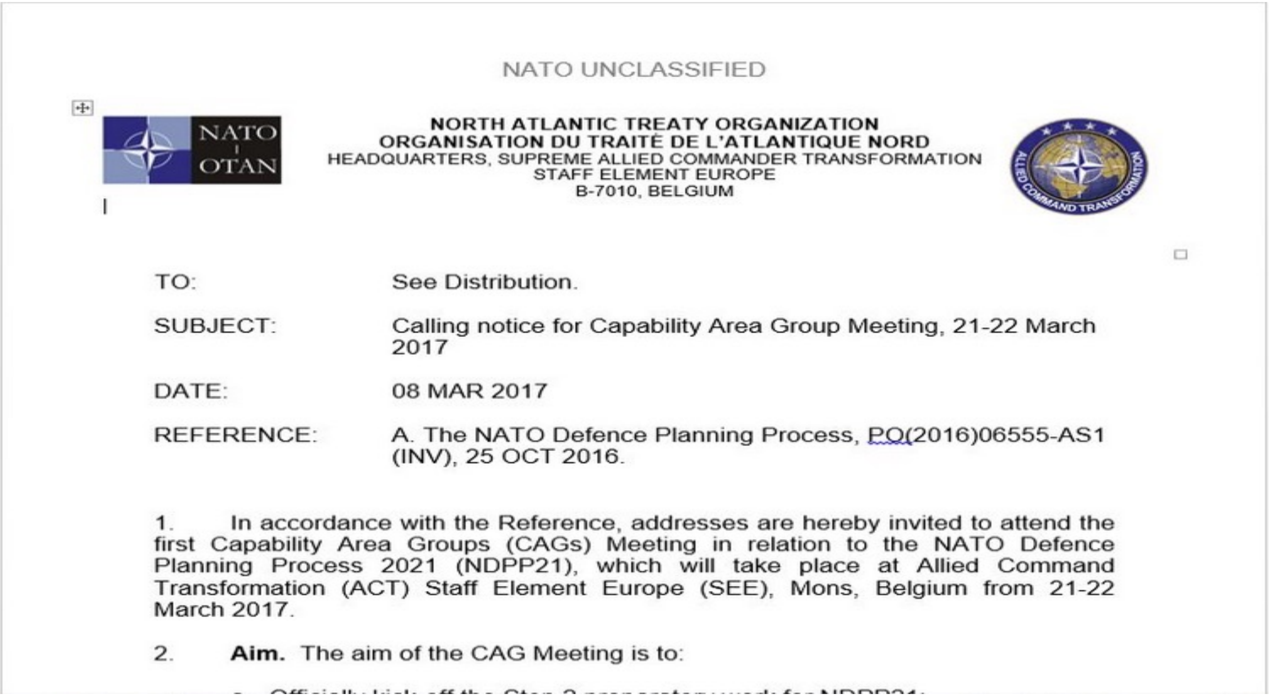


Critical Assets

Baseline

Critical Controls

APT28 + Powershell



NATO UNCLASSIFIED

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS, SUPREME ALLIED COMMANDER TRANSFORMATION
STAFF ELEMENT EUROPE
B-7010, BELGIUM

TO: See Distribution.

SUBJECT: Calling notice for Capability Area Group Meeting, 21-22 March 2017

DATE: 08 MAR 2017

REFERENCE: A. The NATO Defence Planning Process, PO(2016)06555-AS1 (INV), 25 OCT 2016.

1. In accordance with the Reference, addresses are hereby invited to attend the first Capability Area Groups (CAGs) Meeting in relation to the NATO Defence Planning Process 2021 (NDPP21), which will take place at Allied Command Transformation (ACT) Staff Element Europe (SEE), Mons, Belgium from 21-22 March 2017.

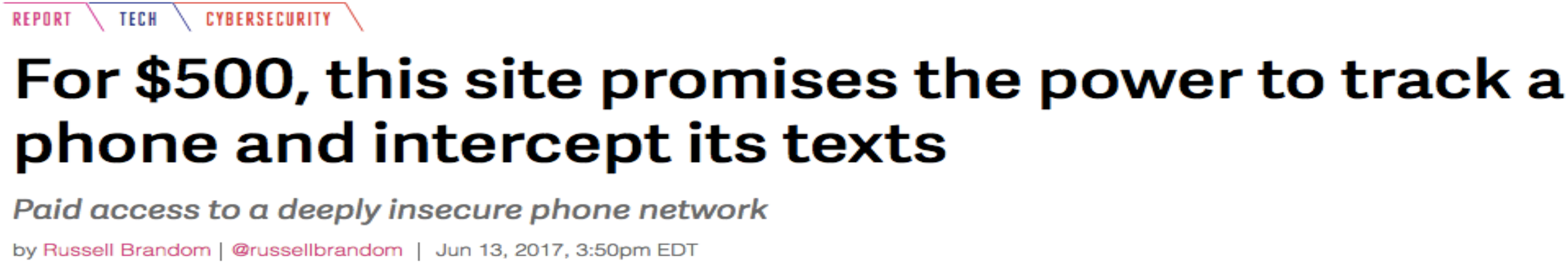
2. **Aim.** The aim of the CAG Meeting is to:

a. Officially kick off the Step 2 preparatory work for NDPP21;

Credential Attack

- FF, IE, Chrome saved credentials
- Recoverable with PowerShell

- SS7 vulnerability



REPORT TECH CYBERSECURITY

For $500, this site promises the power to track a phone and intercept its texts

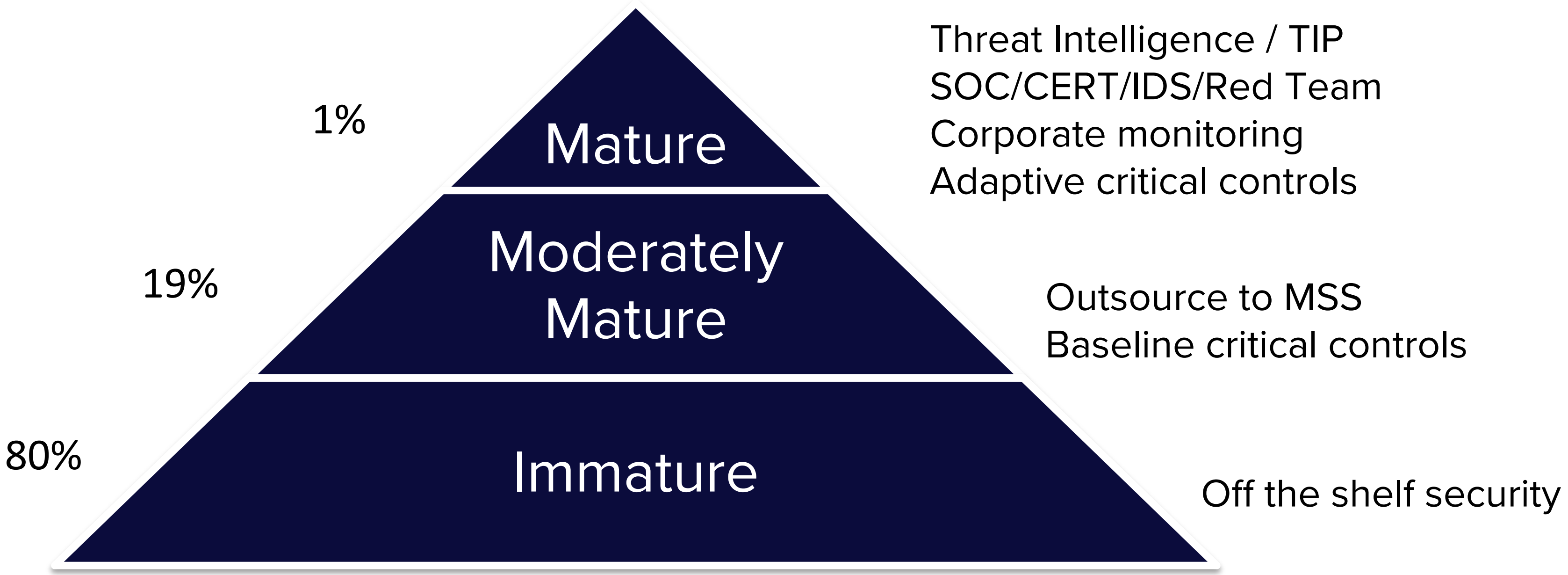
Paid access to a deeply insecure phone network

by Russell Brandom | @russellbrandom | Jun 13, 2017, 3:50pm EDT

Prevention/Detection

- Maximise the benefit of IOCs
  - Timeliness and quality
  - Exchange faster and implement automatically
- TTPs are more stable and valuable
  - Work to do on taxonomy (Att&ck, Sigma)
  - Work to do on translation in actionable code (OpenC2)
- Critical controls have to adapt dynamically
  - New critical vulnerabilities
  - New methods
- Credentials become critical to monitor

Maturity

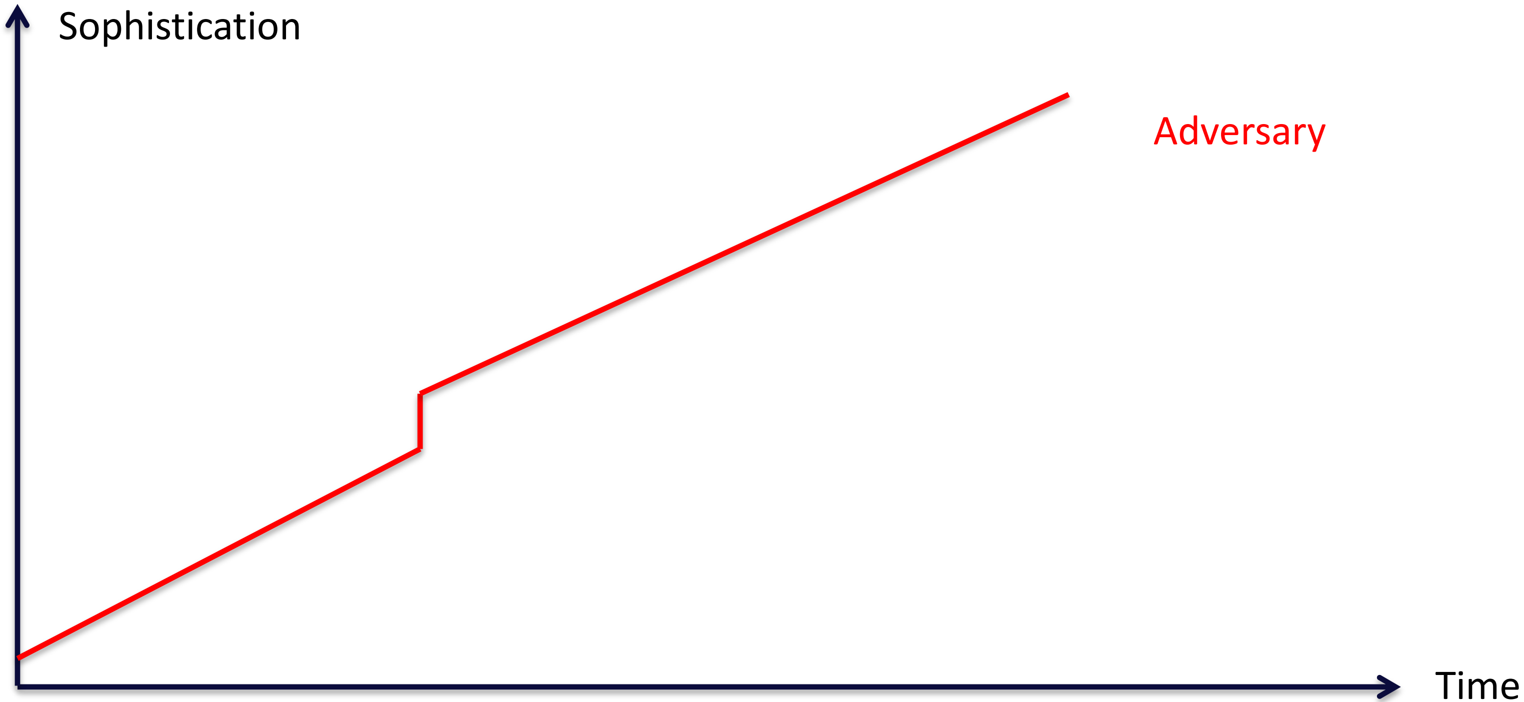


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

Outsource to MSS
Baseline critical controls

Off the shelf security

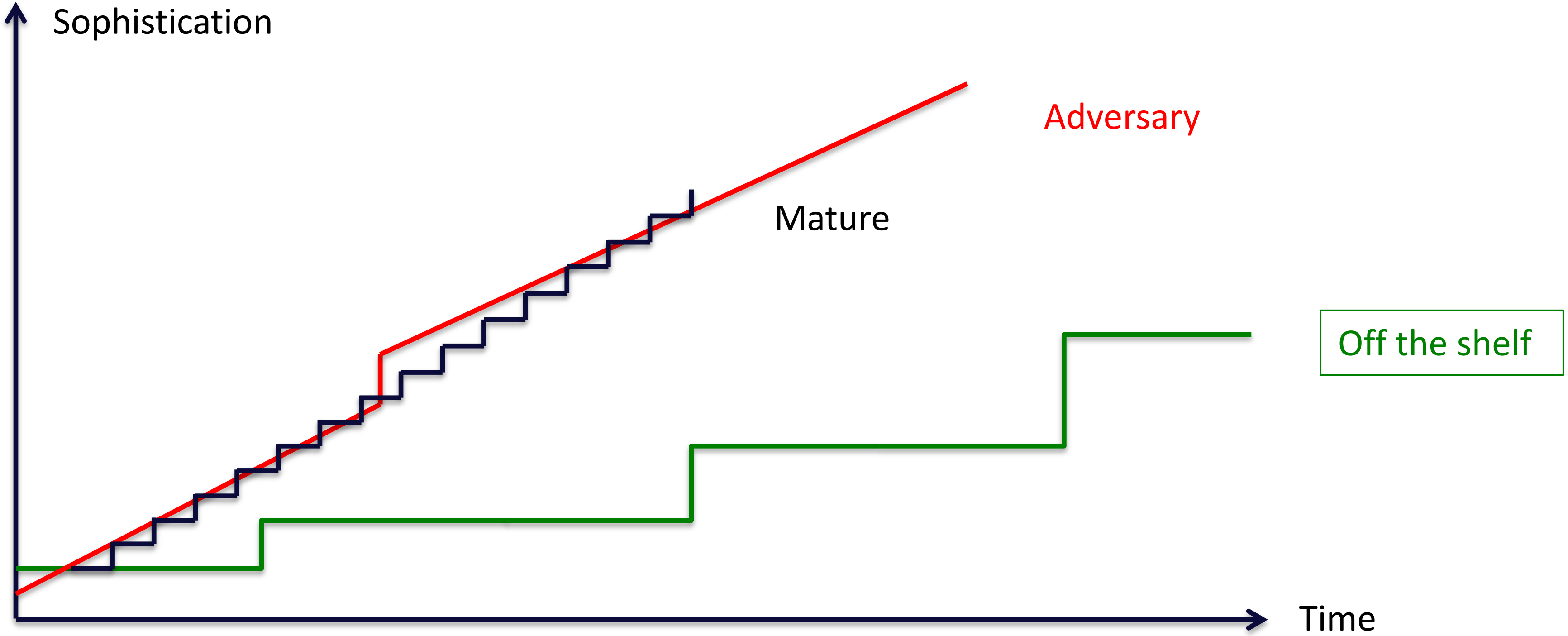
Challenge



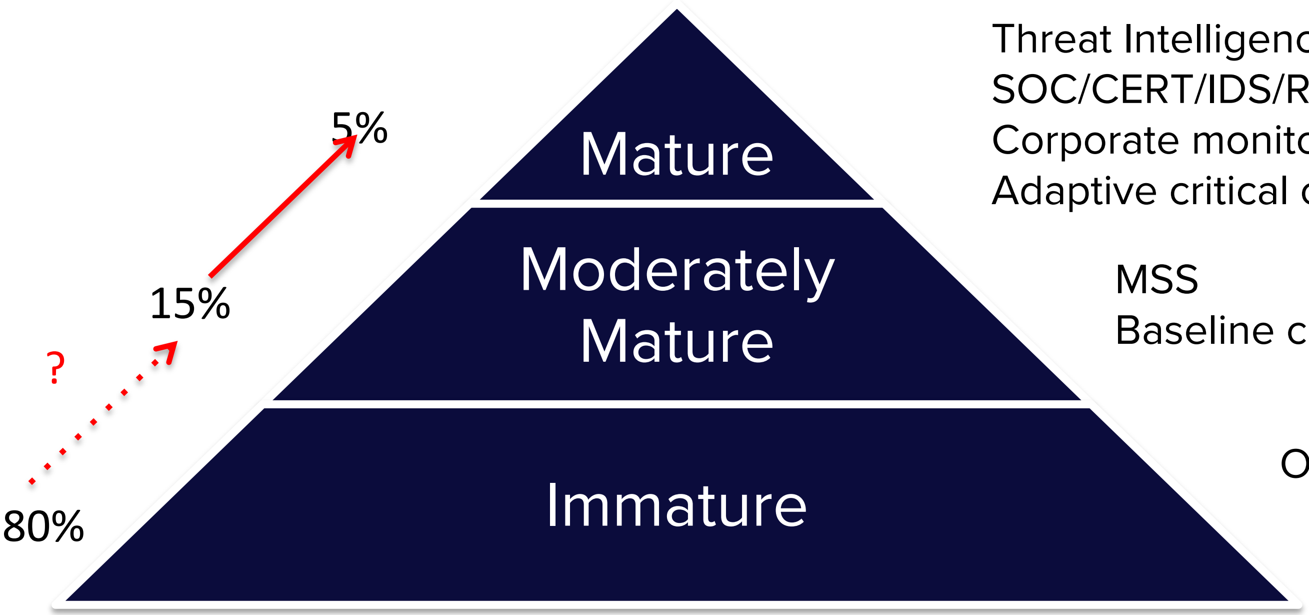
Leakage of Sophisticated Tools

- Espionage & law enforcement tools
  - CIA, NSA etc.
  - Hacking Team
  - NSO
- Penetration and vulnerability testing tools
  - Mimikatz
  - Cobalt Strike
  - Luckystrike
  - Responder
  - Metasploit

Gap



Opportunity



5%

Mature

15%

Moderately Mature

?

80%

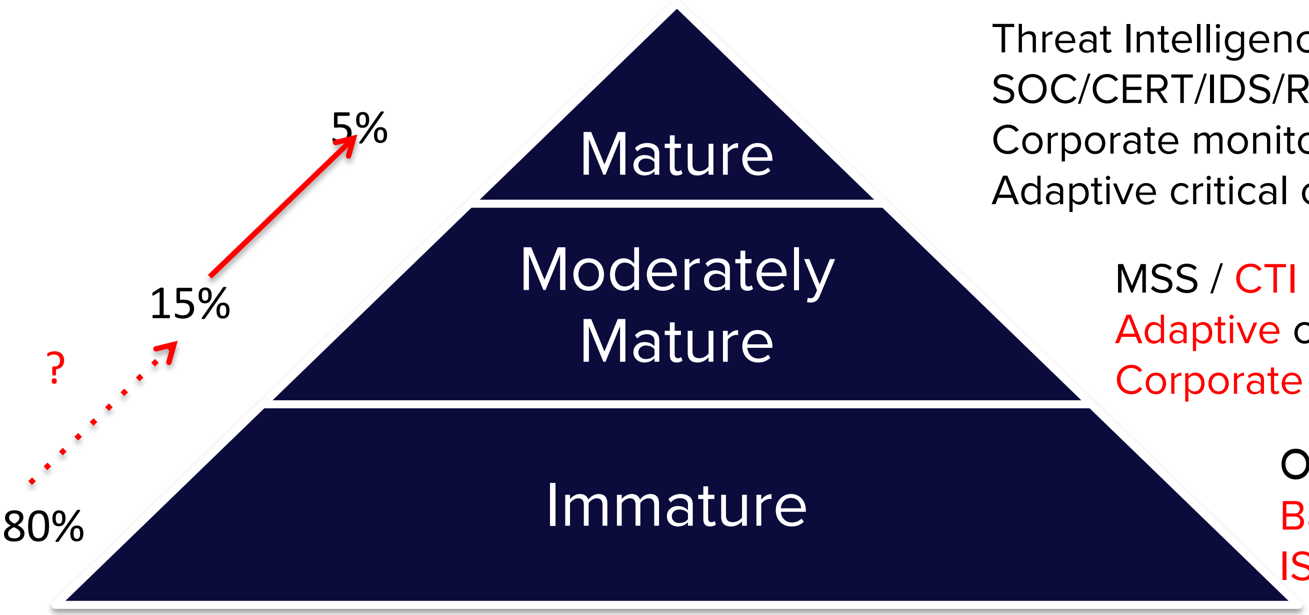
Immature

Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

MSS
Baseline critical controls

Off the shelf security

Opportunity

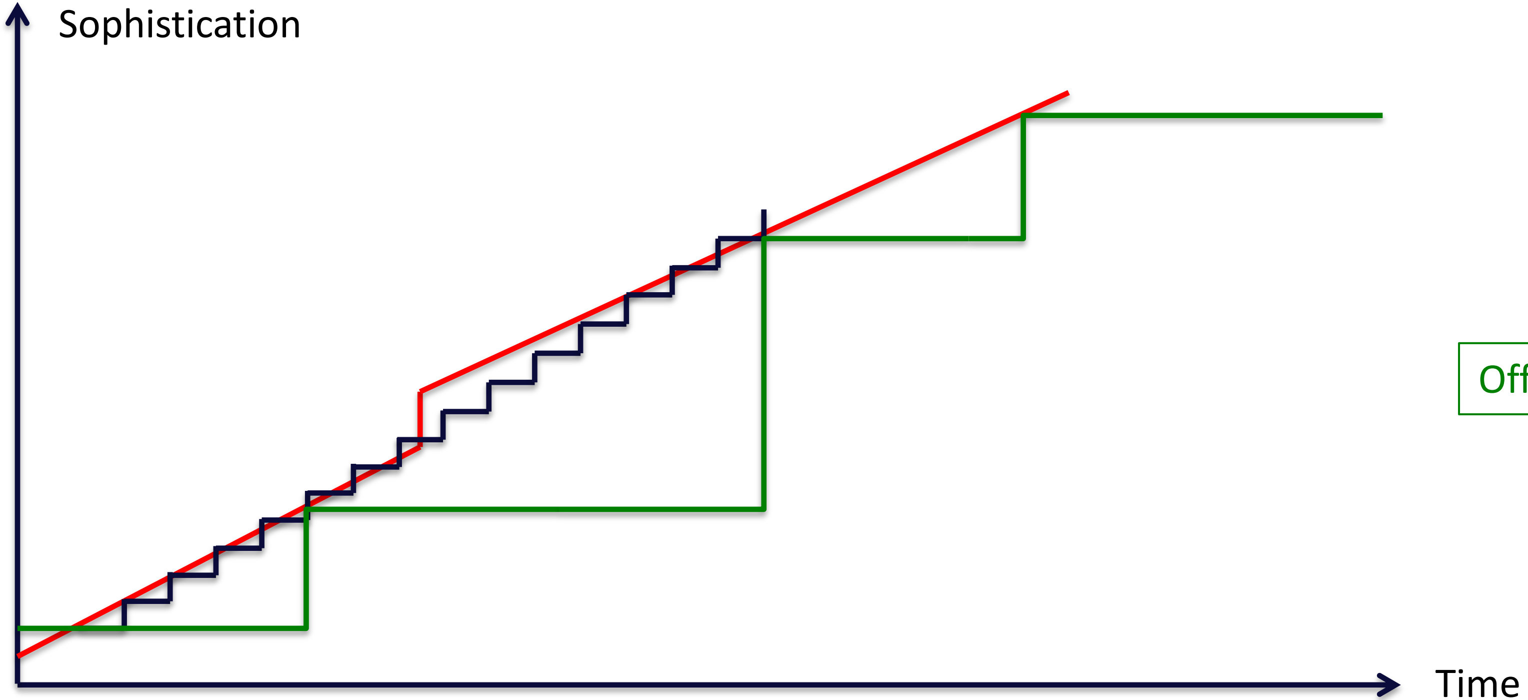


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

MSS / CTI Fusion Center
Adaptive critical controls
Corporate monitoring

Off the shelf security
Baseline critical controls
ISP protection

Gap



Off the shelf

Opportunity

ISP/Cloud with security built in

- IDS/IPS/Firewall + indicators/rules
- Secure DNS, DMARC
- Scanning service for vulnerabilities/misconfiguration
- Block/remove rogue devices/systems
- Corporate monitoring – domains/credentials
- Awareness raising
- Baseline controls

Opportunity

Community

- Threat monitoring
- Curated IOCs and Hunting rules
- Taxonomies, standards
- Adaptive critical controls
- Use cases, playbooks, tools

Just One More Thing

Any information relating to an ***identified*** or ***identifiable natural*** person

- IP, DNA, fingerprint, credit card, username, address, email address, phone number…

- Processed by an ***establishment in the EU***
- Or related to ***data subjects in the EU***
- Or related to ***behavior taking place in the EU***

- ***Even if at no cost***

Lawfulness

GDPR spells out six lawful grounds:

a. Consent
b. Contract
c. Compliance with a legal obligation
d. Vital interests of a person
e. Task in the public interest
f. Legitimate interest
    - ➢ Recital 49

Recital 49

- Processing of personal data to ***the extent strictly necessary and proportionate*** for the ***purposes of ensuring network and information security*** … constitutes a ***legitimate interest***.
- No need for consent of the data subjects.
- Purpose of the processing and its justification should be documented
- Precautions needed to ***avoid use for other purposes***.

Take Aways

- Threat landscape becomes ever more challenging
- Optimise the use of CTI in your infrastructure

- Strengthen the community

- Raise the bar
- But not only for the 1%…

Thank You

Don’t Hide The Risk, Manage It

freddy.dezeure@gmail.com
dezeuref@gmx.com
freddy.dezeure@protonmail.com