Intel Driven Detection / Prevention

September 2017

About Me

- Board EclecticIQ
- Advisory Board Spycloud, Intel471, Phantom Cyber
- Six years Head of CERT-EU
  - Set up from greenfield, protecting 100.000 users in 60 organizations
- Thirty years the European Commission
  - COO, CRO (3000 scientists)
  - IPR protection and valorization (patents, spin offs, seed capital)
  - Internal and external audit
- Five years as a CIO in private industry

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

(Not)Petya June 2017

- Initial distribution via MeDoc
- Disruptive intent
- Massive economic impact
- Disruption

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"

Stealthier

- Emails bypassing protective layers
  - Mimicking trusted parties (spoofing, typosquatting, springboarding)
  - Unpatched vulnerabilities (Flash, Java, MSFT, Apache)
  - Non-active or low-active content (JavaScript, Macros)
  - Encrypted, password protected, attachments
- Using legitimate OS components (PowerShell, WMI)
- Using legitimate credentials

- Prevention becomes more and more difficult

(Not)Petya

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

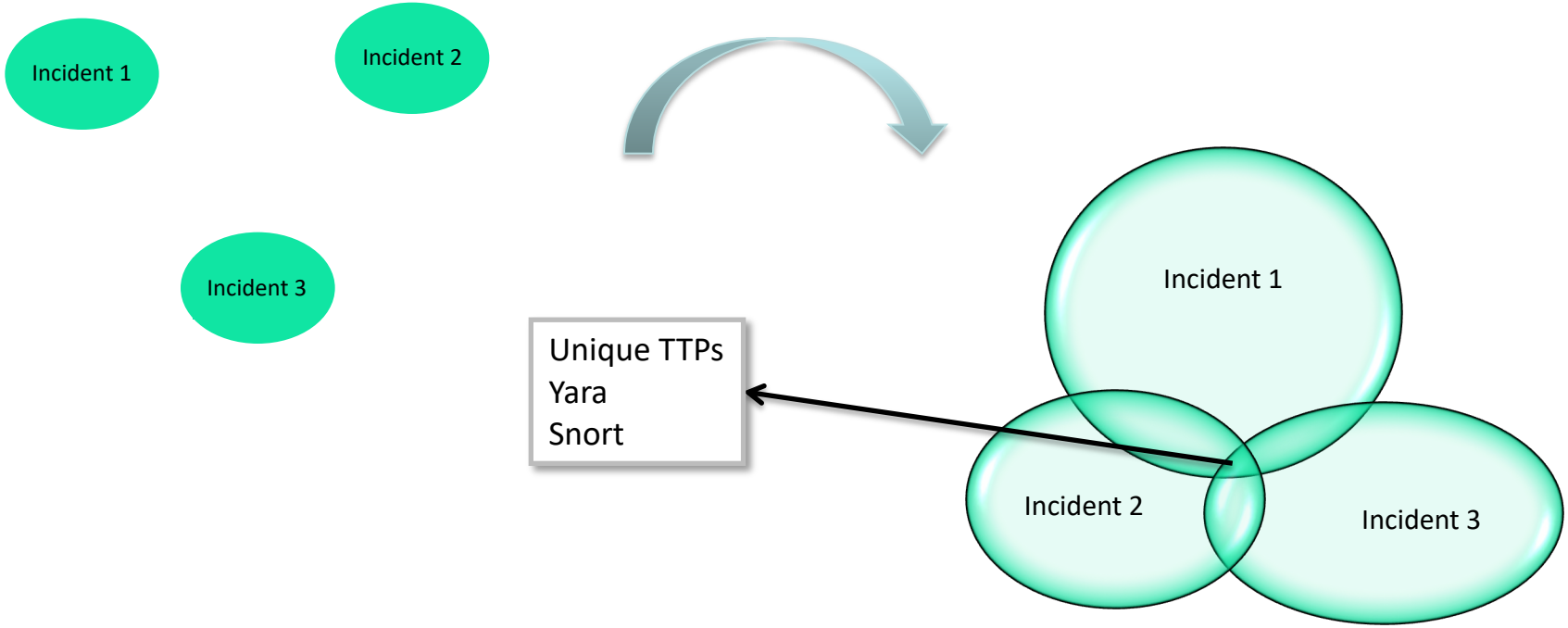
An unknown actor had stolen the credentials of an administrator at M.E.Doc. They logged into the server, acquired root privileges and then began modifying the configuration file for the NGINX web server. We were unable to recover the nginx.conf file, as it was subsequently overwritten, but additional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

IOC Challenges

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

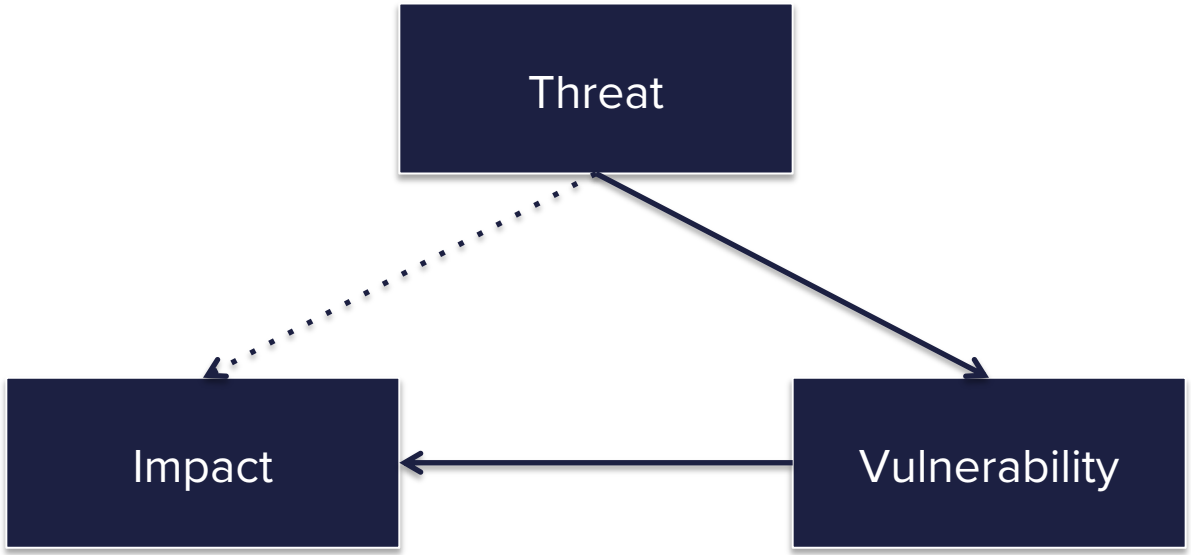
- Detection becomes more and more difficult

TTPs are more stable



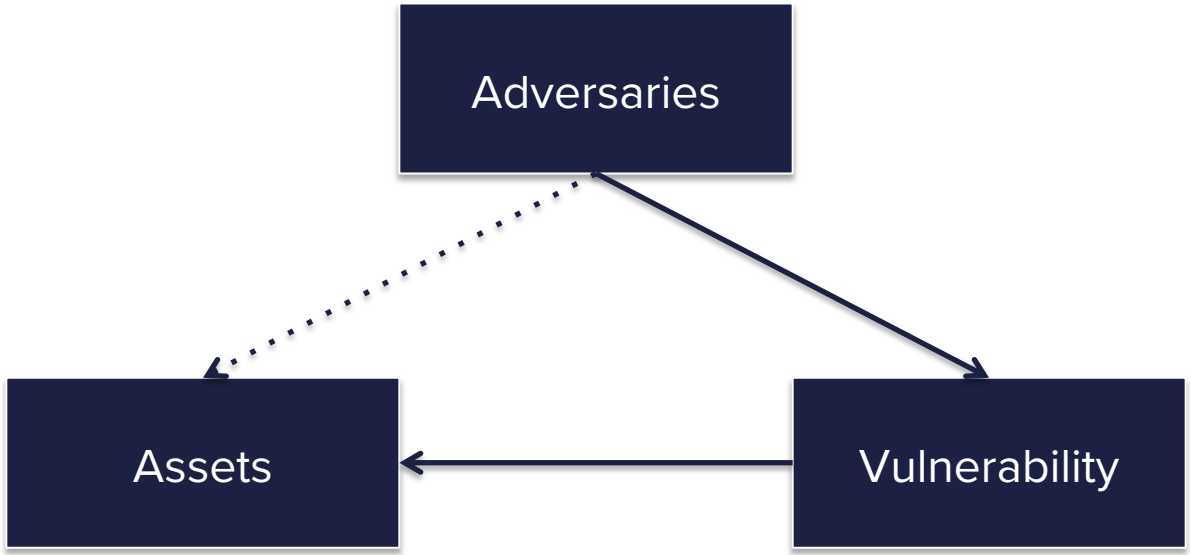
Risk

Threat x Vulnerability x Impact



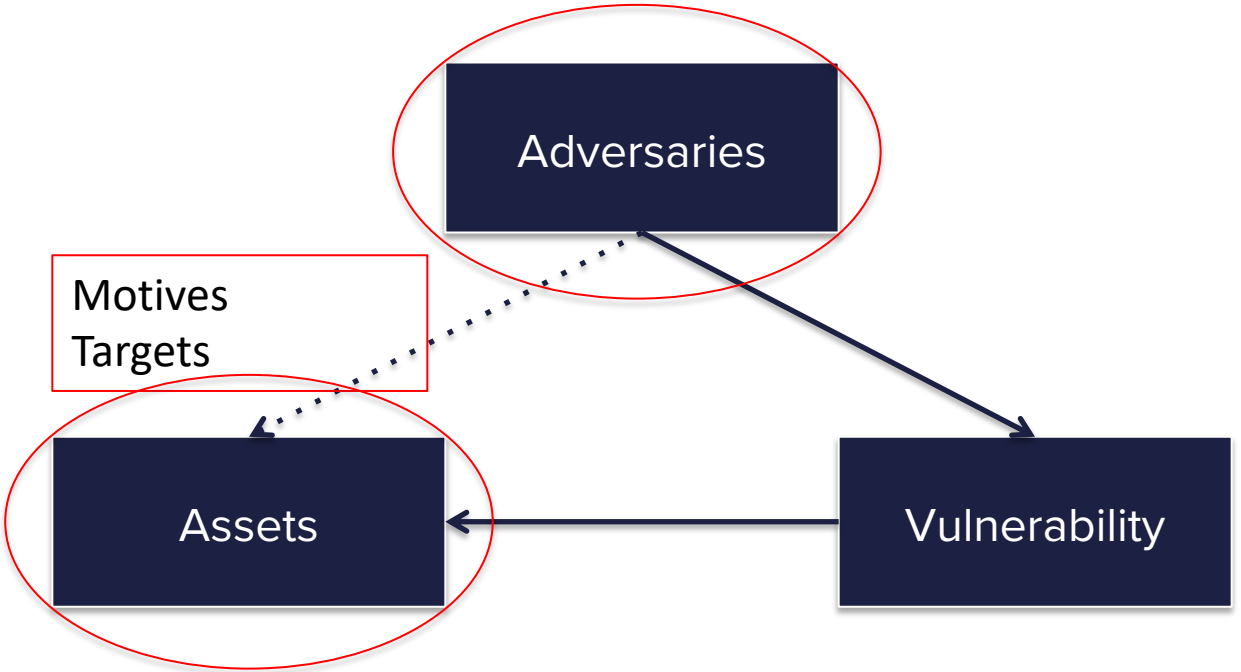
Risk

Threat x Vulnerability x Impact



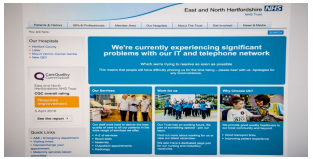
Threat Intelligence

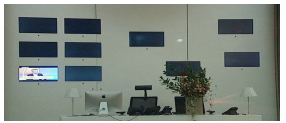
Threat x Vulnerability x Impact



Motives/Targets

- Money
  - Targeted ransomware, blackmailing
  - Diverting financial transactions
  - Benefitting from inside information
  - Market manipulation
- Position
  - Compete (IPR, business information)
  - Oppress political adversaries, manipulate press, opinion
- Disruption
  - Strategic
  - (Terrorism)





Inside Information

SEC hacked for possible 'illicit' trading gains

Probe ordered after breach of Edgar online information filing system

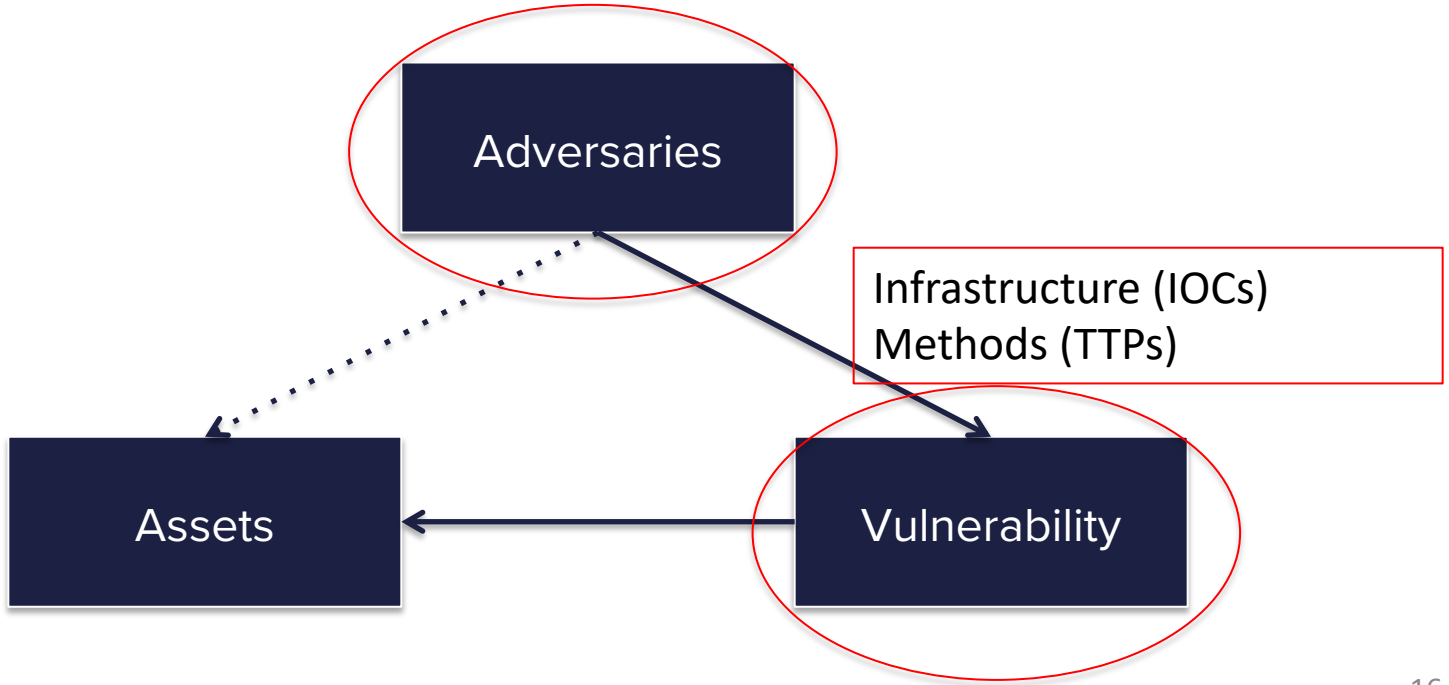
© Joshua Roberts/Bloomberg

1 Save to myFT

7 HOURS AGO by David J Lynch in Washington

Threat Intelligence

Threat x Vulnerability x Impact



Credential Attack

- FF, IE, Chrome credentials recovered 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

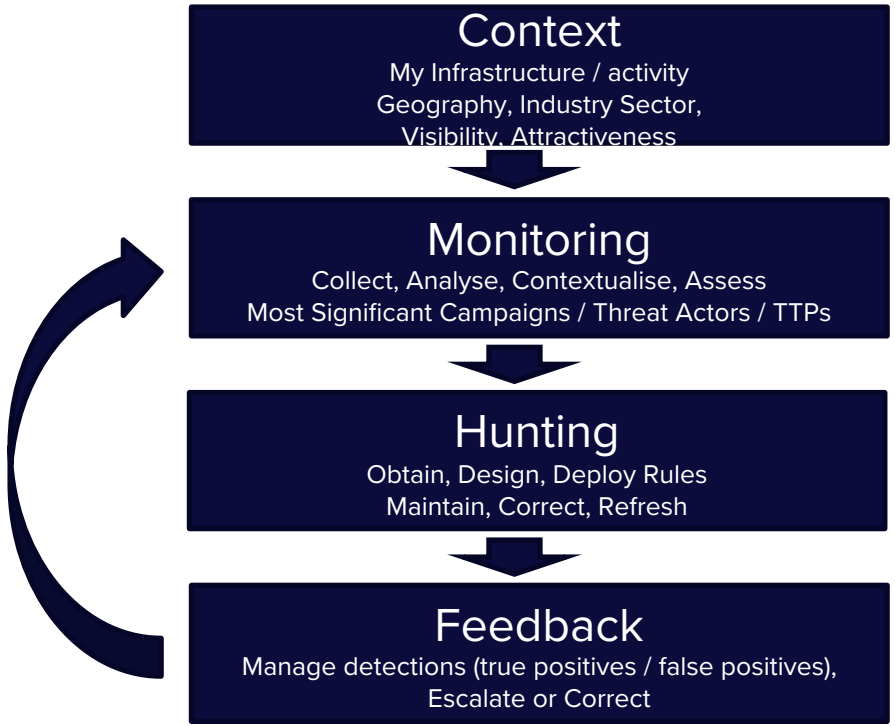
Observe

Key Questions

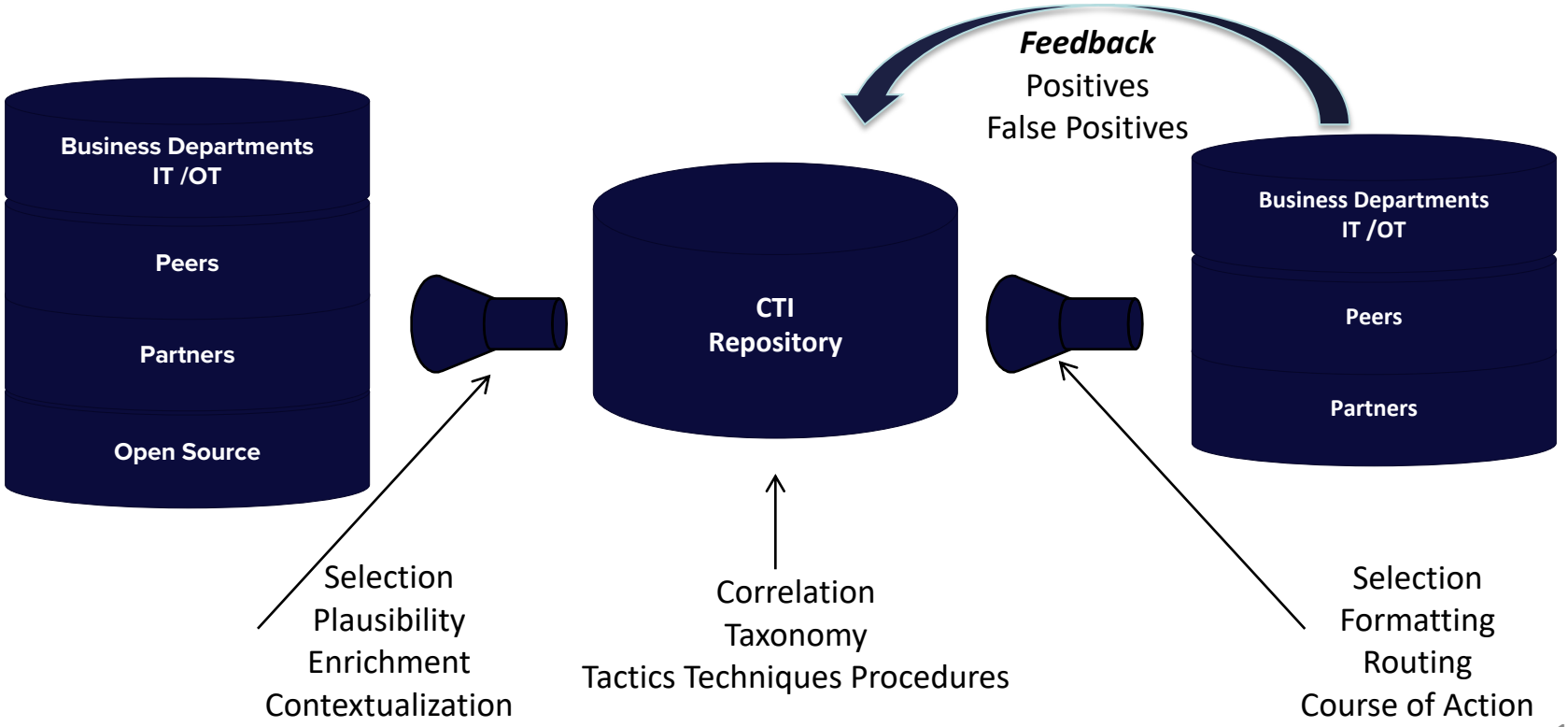
- Who?
- What?
- Why?
- How?
- When?
- Does it matter to us?

Risk *Management*

- From data to intelligence
- Serving a purpose
- Not all risks are equal
- Situation is not static

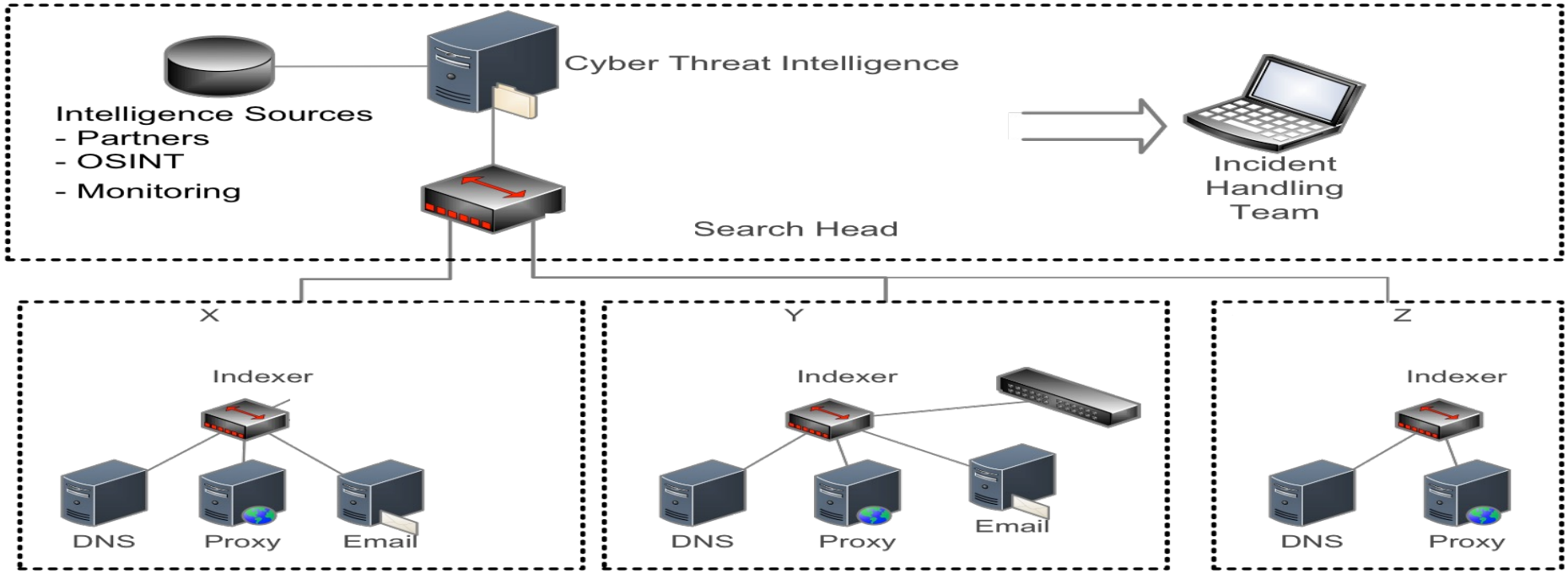


CTI Process

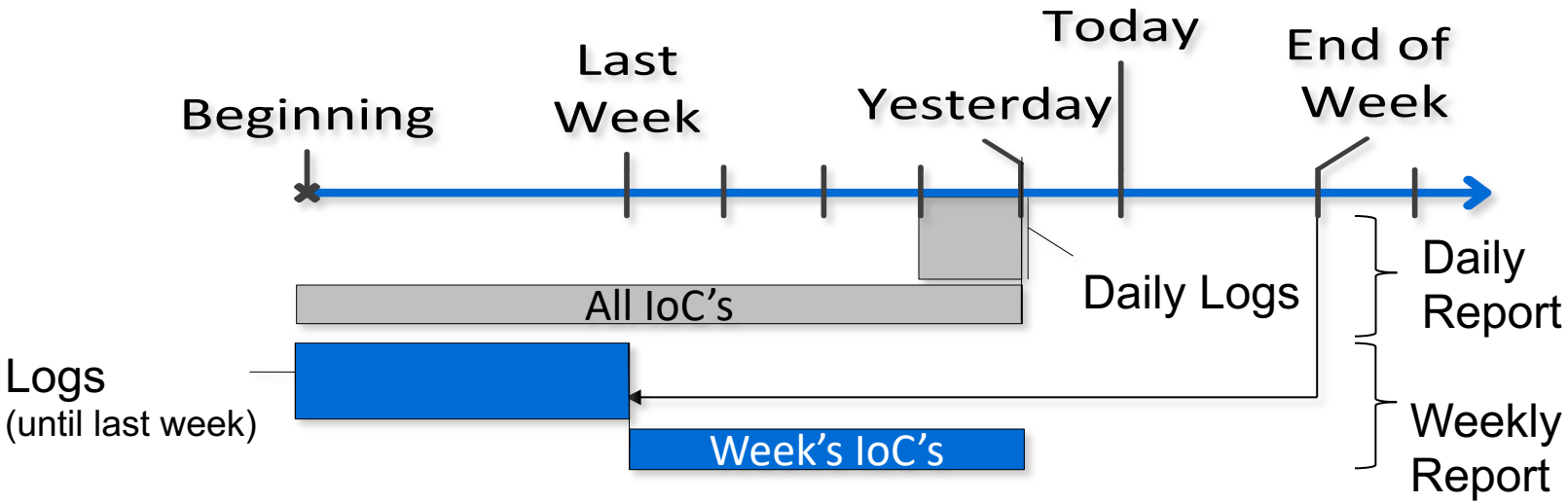

Feedback
Positives
False Positives
Business Departments
IT /OT
Peers
Partners
Open Source
CTI
Repository
Business Departments
IT /OT
Peers
Partners
Selection
Plausibility
Enrichment
Contextualization
Correlation
Taxonomy
Tactics Techniques Procedures
Selection
Formatting
Routing
Course of Action

Contextualisation

Detection


Cyber Threat Intelligence
Intelligence Sources
- Partners
- OSINT
- Monitoring
Incident Handling Team
Search Head
X
Indexer
DNS
Proxy
Email
Y
Indexer
DNS
Proxy
Email
Z
Indexer
DNS
Proxy

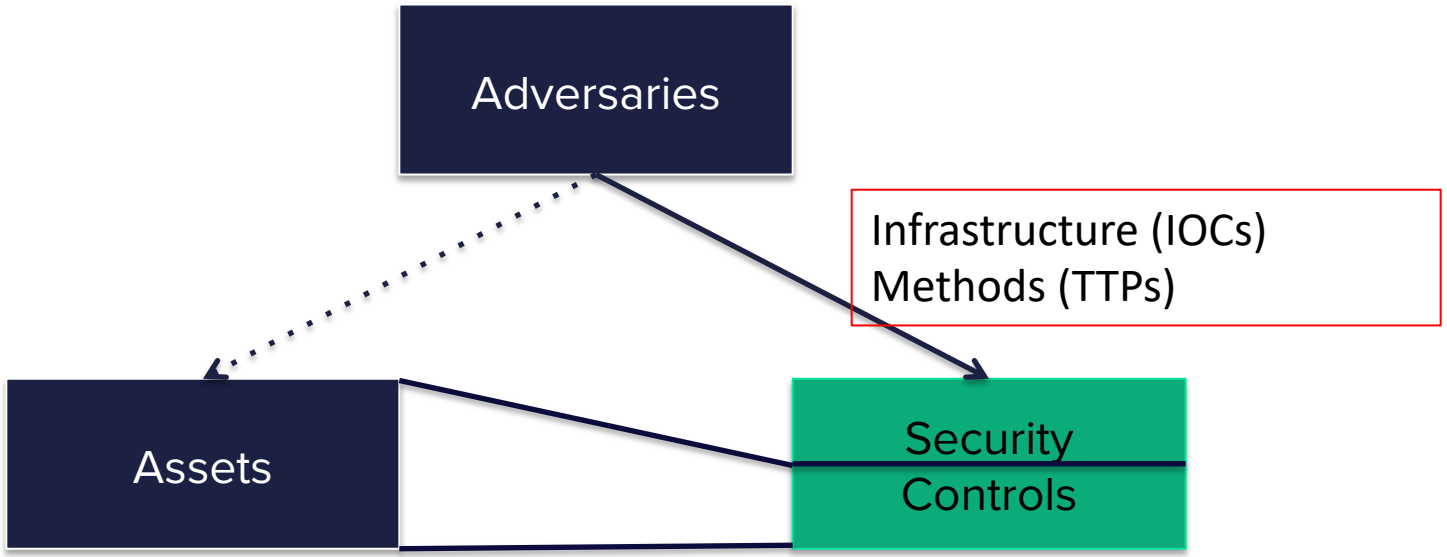
Intelligence Correlation



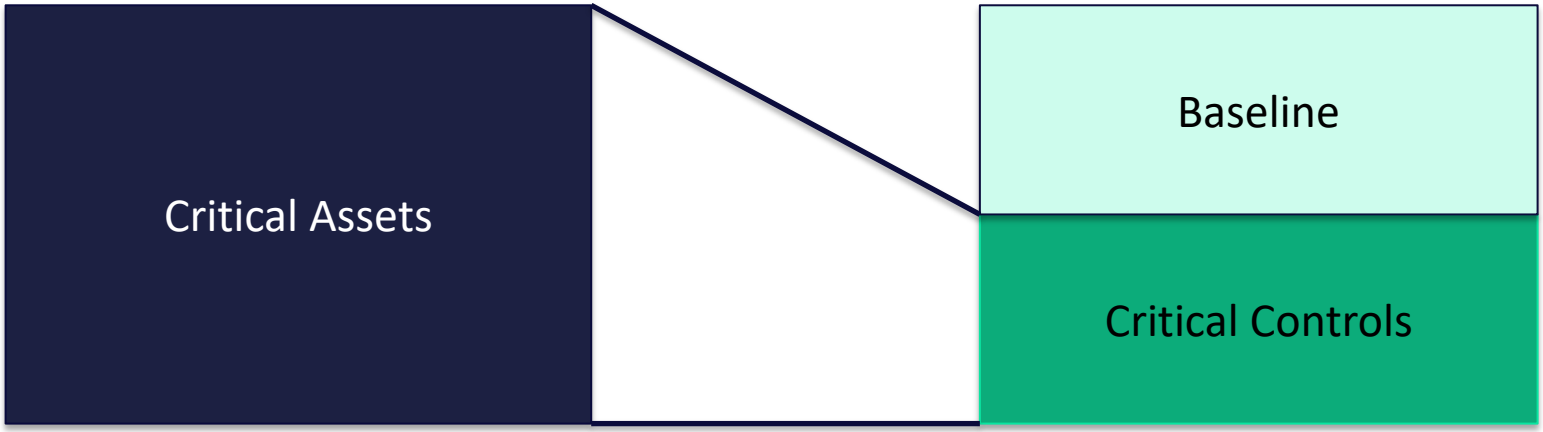
* Simplified for the presentation

Mitigate Risk

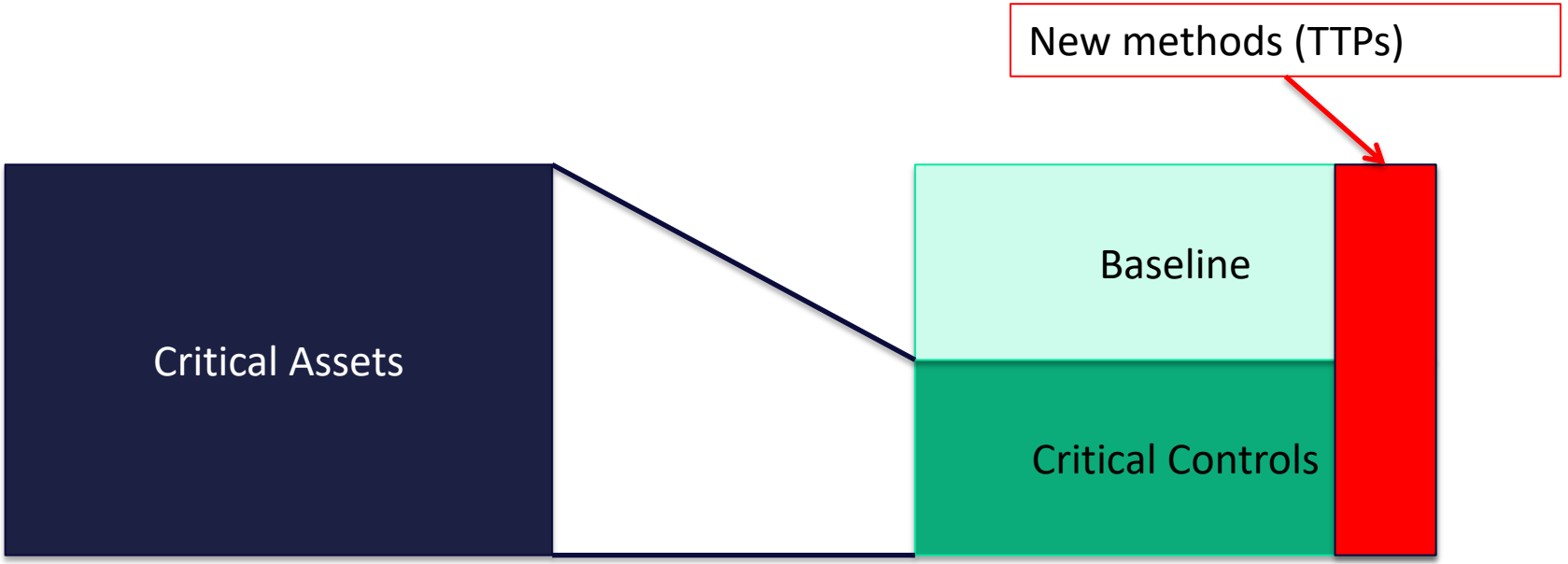
Threat x Vulnerability x Impact



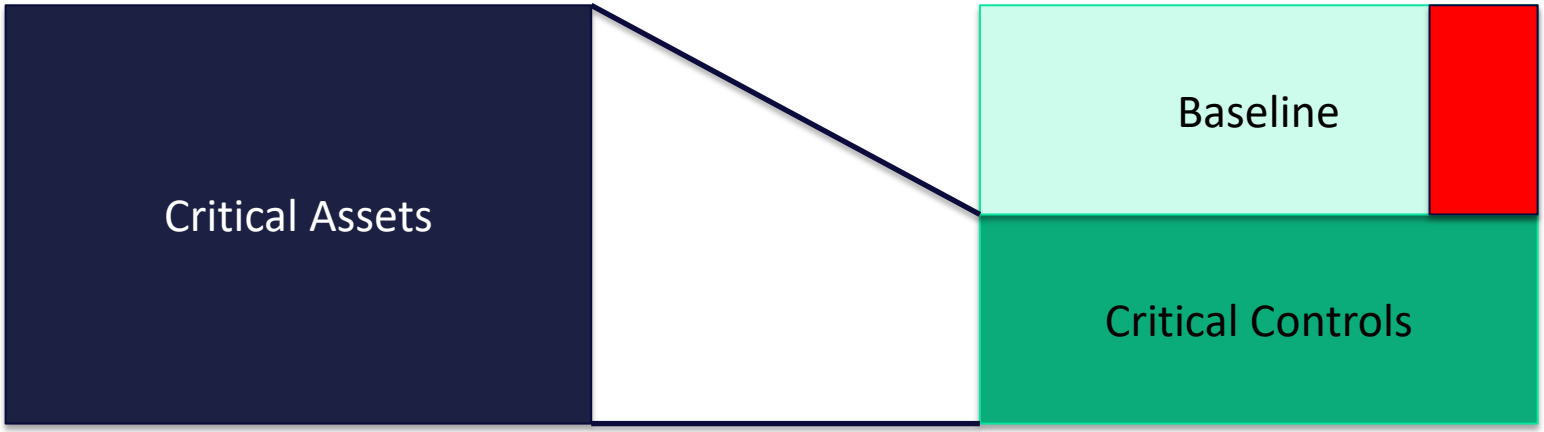
Prevention



Check Against New TTPs



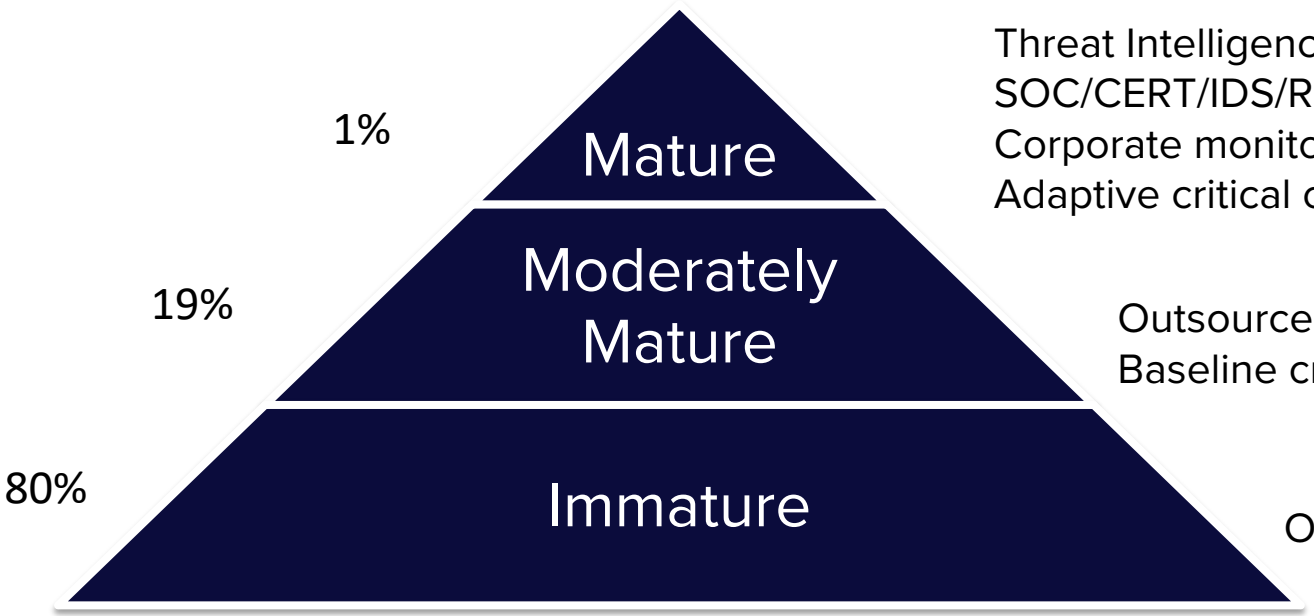
Adapt



Prevention/Detection

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

Maturity

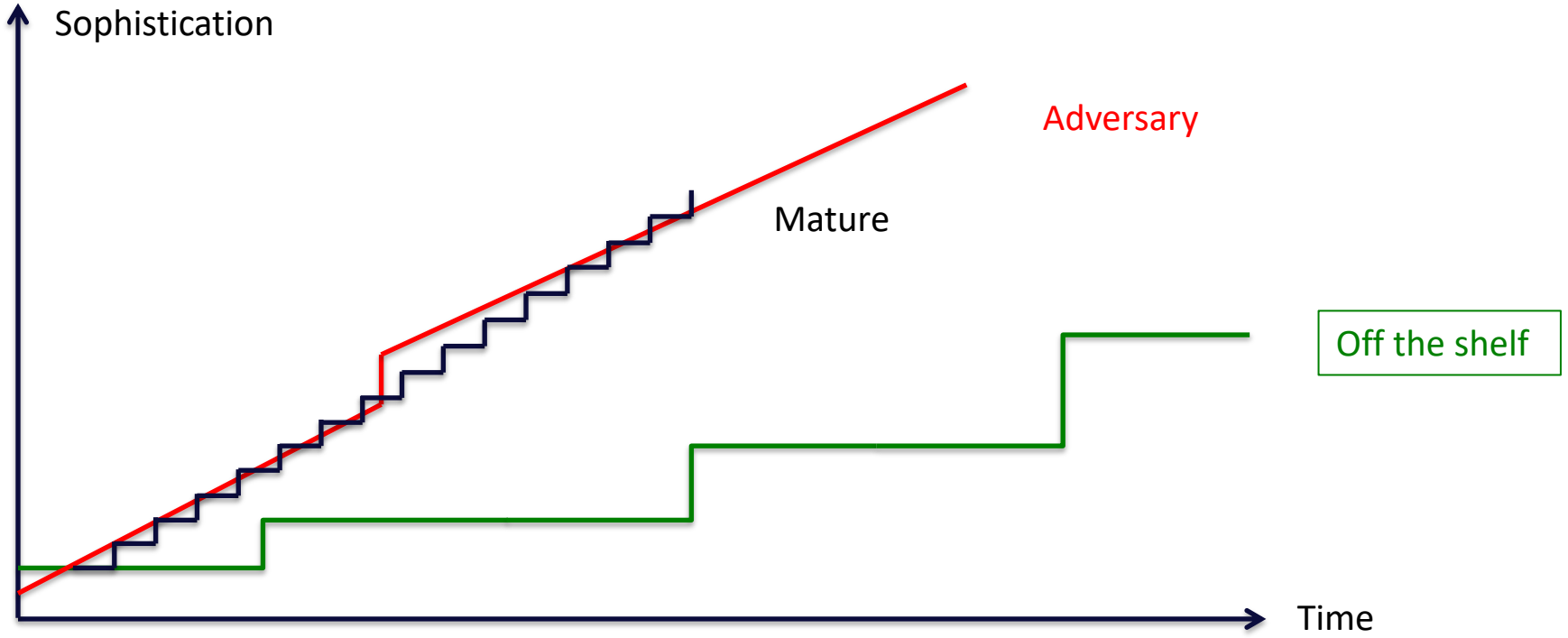


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

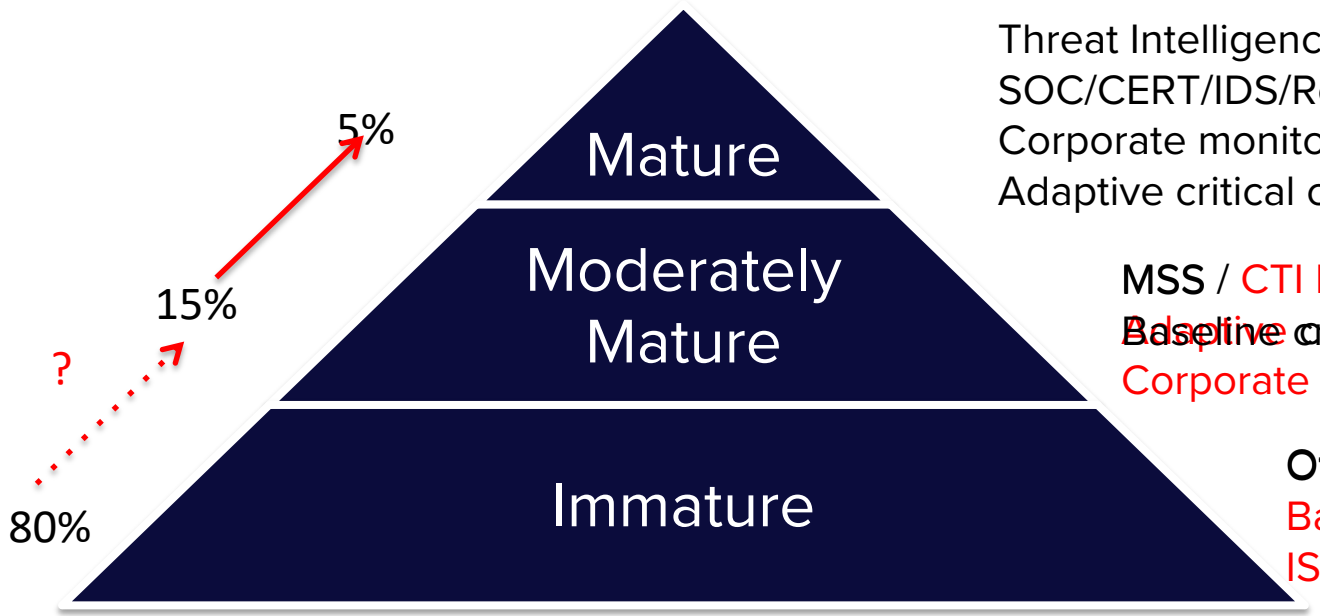
Outsource to MSS
Baseline critical controls

Off the shelf security

Gap



Opportunity

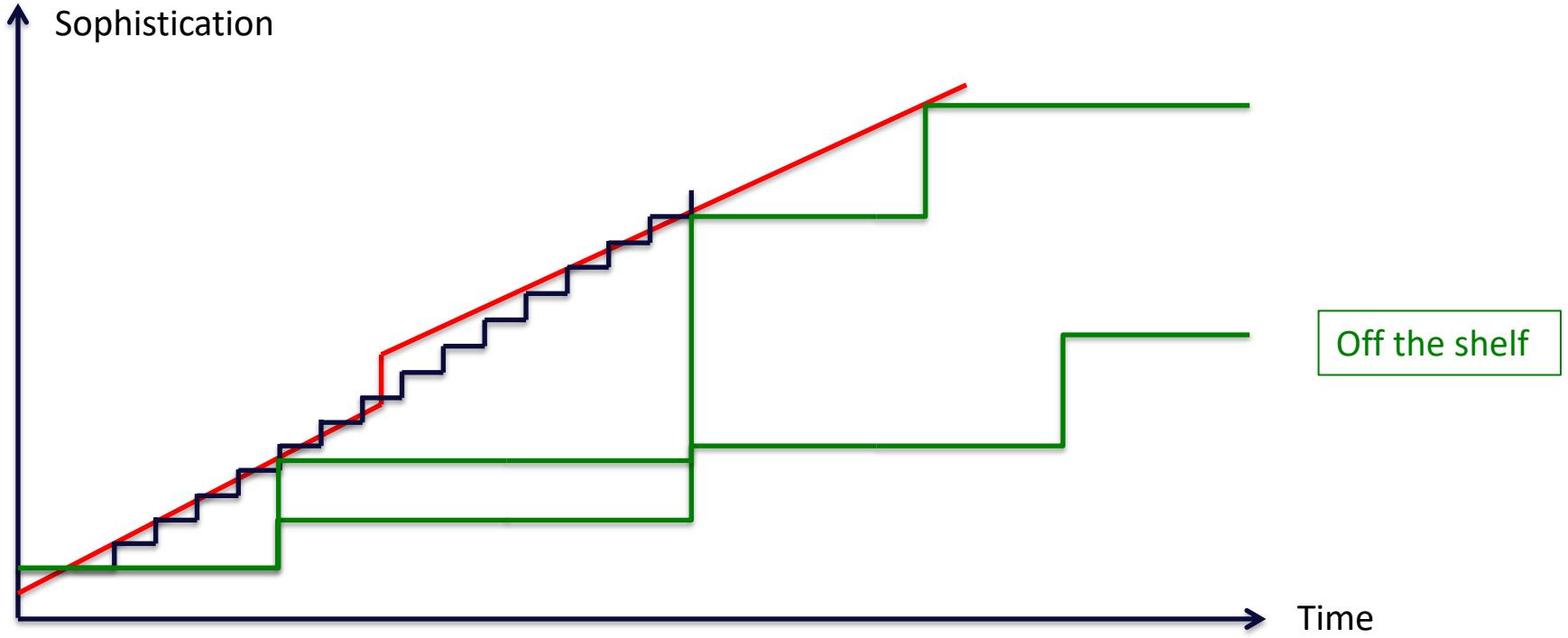


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

MSS / CTI Fusion Center
Baseline critical controls
Corporate monitoring

Off the shelf security
Baseline critical controls
ISP protection

Gap



Opportunity

ISP/Cloud with security built in / certified

- 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: GDPR

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***

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 to ***avoid use for other purposes***.

Take Aways

- Threat landscape becomes ever more challenging
- Even more so for less mature organisations

- Integrate cyber into your normal risk management
- 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