FREDDY DEZEURE

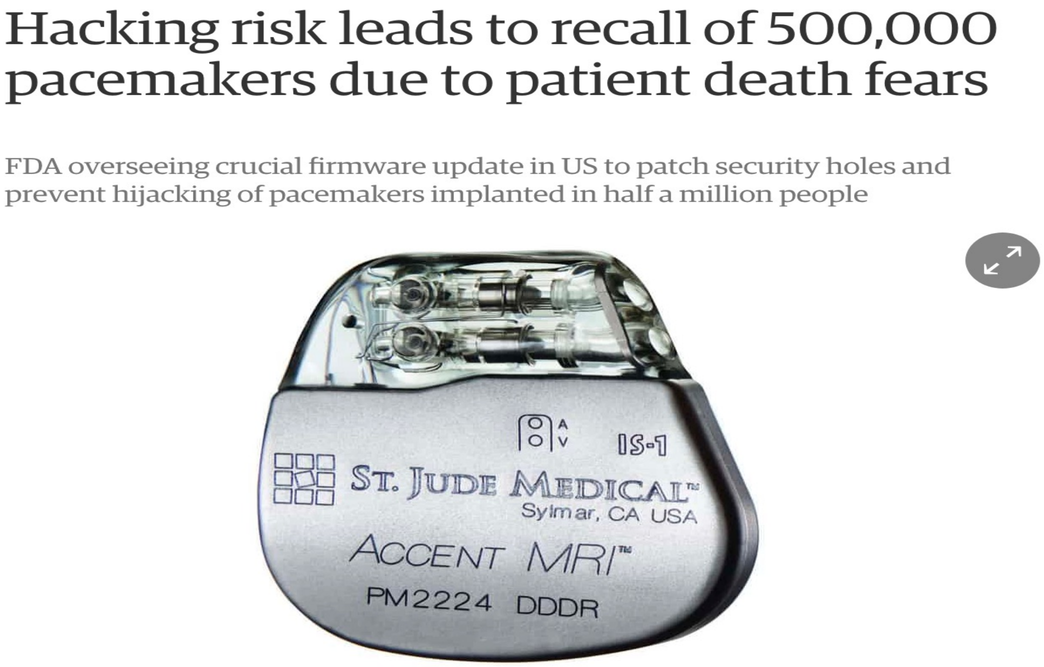
What's Next ?

Risks and Opportunities

September 2017

Agenda

- General context
- Risks
- Opportunities
- One More Thing



Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

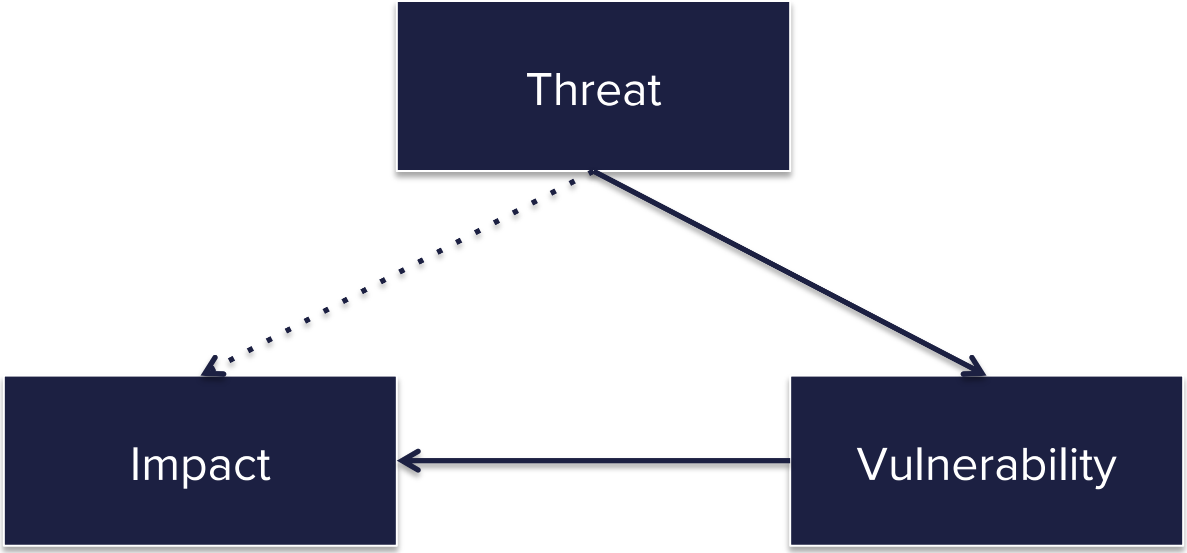
FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

General Context

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

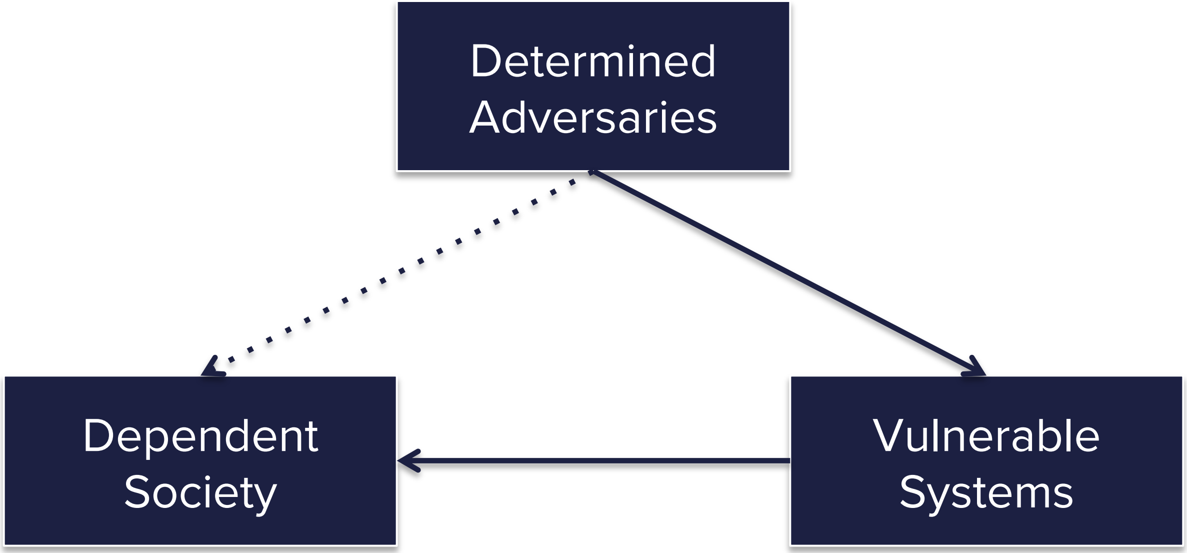
Risk

Threat x Vulnerability x Impact



Risk

Threat x Vulnerability x Impact



Impact

- (Not)Petya - 28 June 2017
- Initial distribution via MeDoc
- Disruptive intent
- “non-targeted”
- Massive economic impact
- Disruption

Impact

Maersk/APM

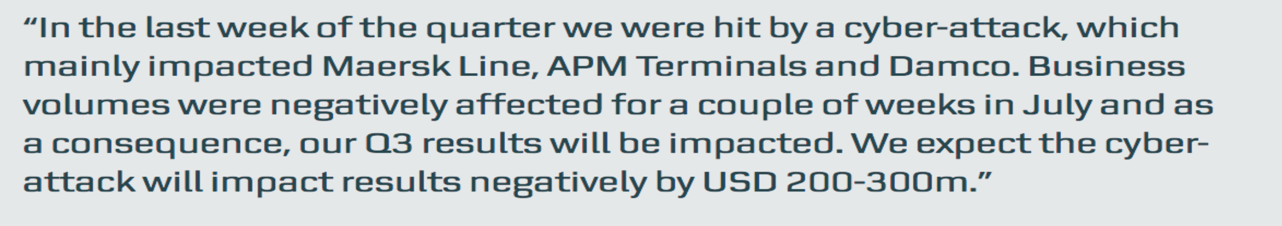
- 17 container terminals disrupted for days
- Loading and unloading impossible because of uncertainty of the shipments
- Delays down the logistic chain
- Perishable goods lost?

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?

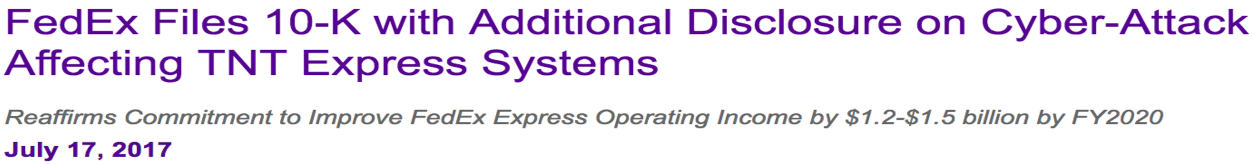
Impact

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

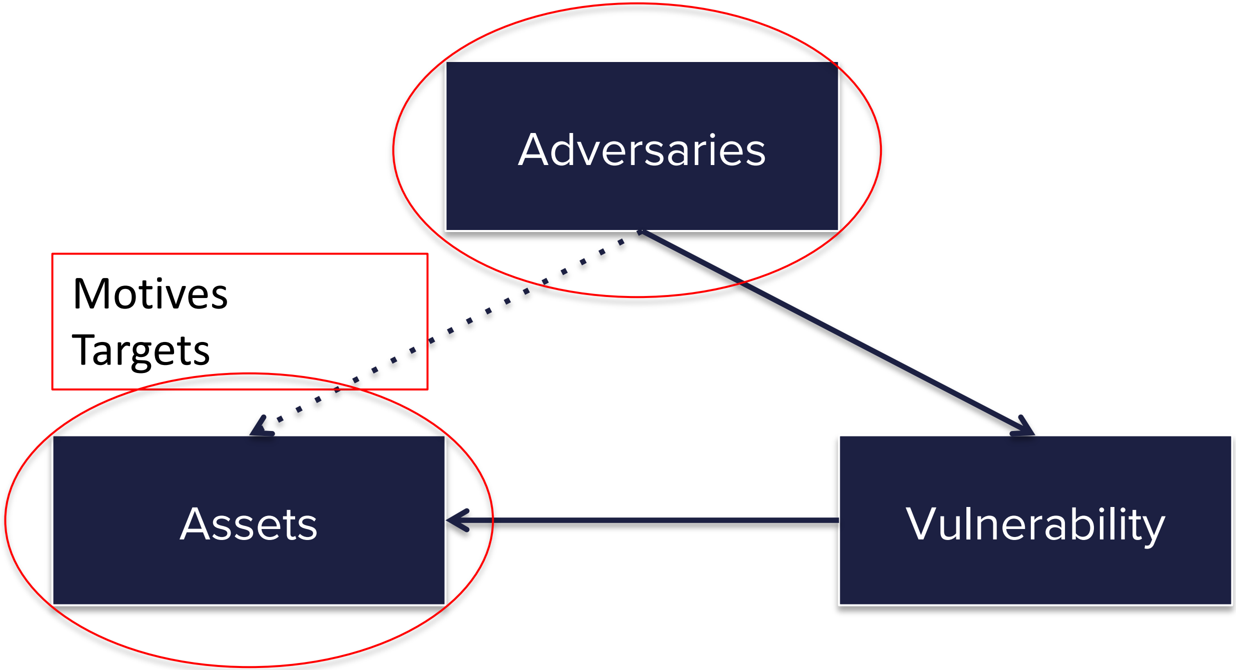
July 17, 2017

"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"

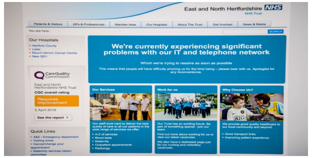
Impact

Threat x Vulnerability x Impact



Motives/Targets

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



East and North Hertfordshire NHS
NHS Trust

You are here:

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

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.

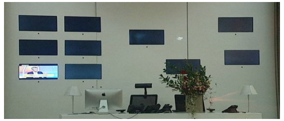
Find out more about working for us or view our latest vacancies.

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

Why Choose Us?

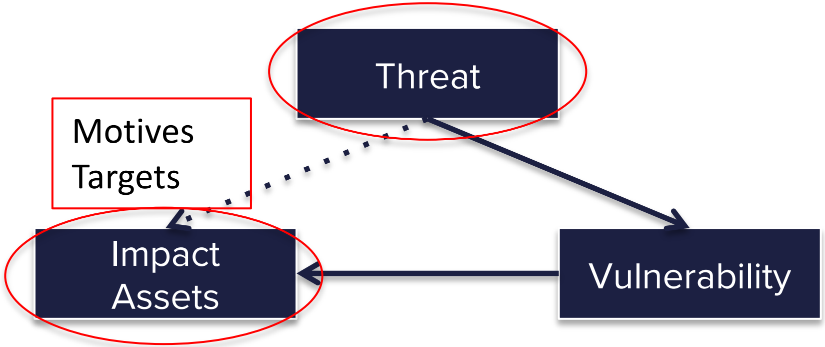
We provide good quality healthcare to our local community and beyond.
- Good transport links
- Improving patient experience

- Position
  - Compete (IPR, business information)
  - Oppress political adversaries, manipulate press, opinion



- Disruption
  - Strategic
  - (Terrorism)

Opportunity



- Translate cyber risk into business risk
- Include in the normal business processes
- Raise awareness and train your C- and Board level
- Protect critical infrastructure according to NIS
- Exchange information in sectorial ISACs

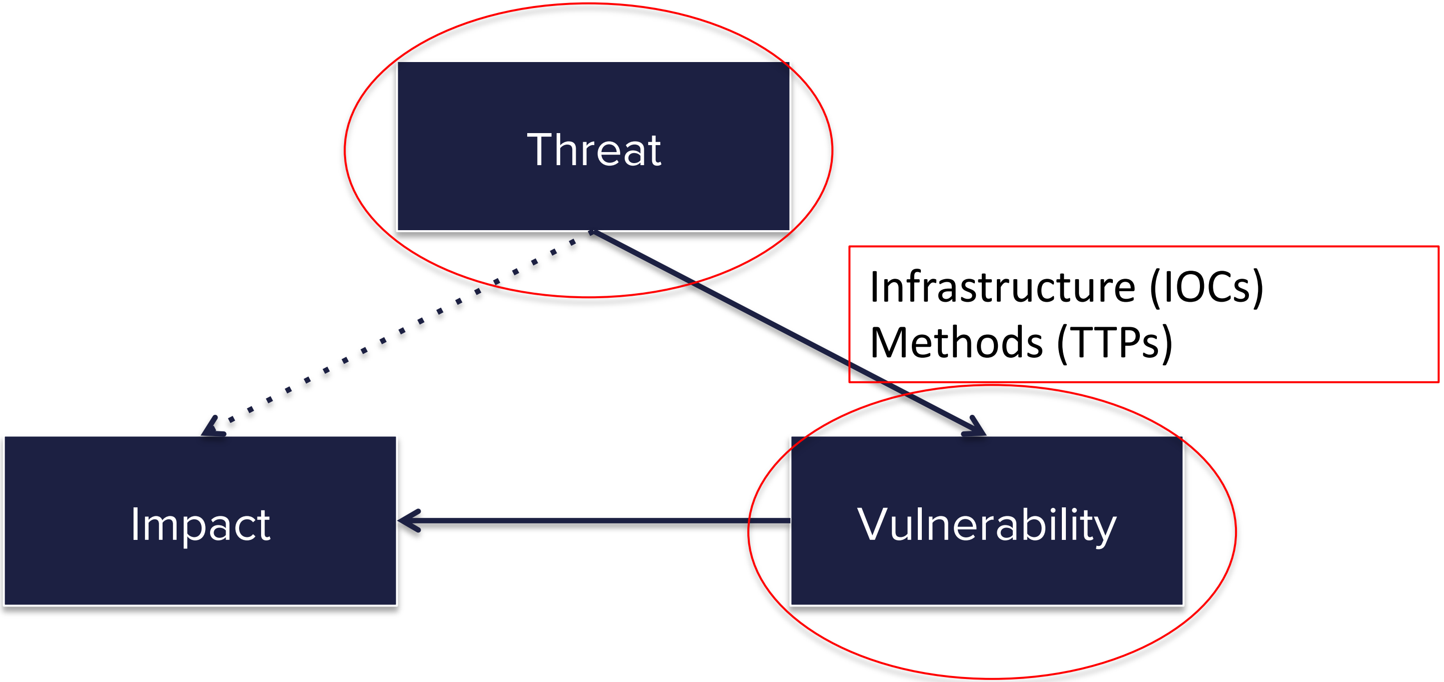
COM(2016) 410 final

"The Commission will:

- foster the emergence of European cooperation of Sectoral Information Sharing and Analysis Centres, support their collaboration with CSIRTs and seek to address barriers that prevent market participants from sharing information;"

Vulnerability

Threat x Vulnerability x Impact



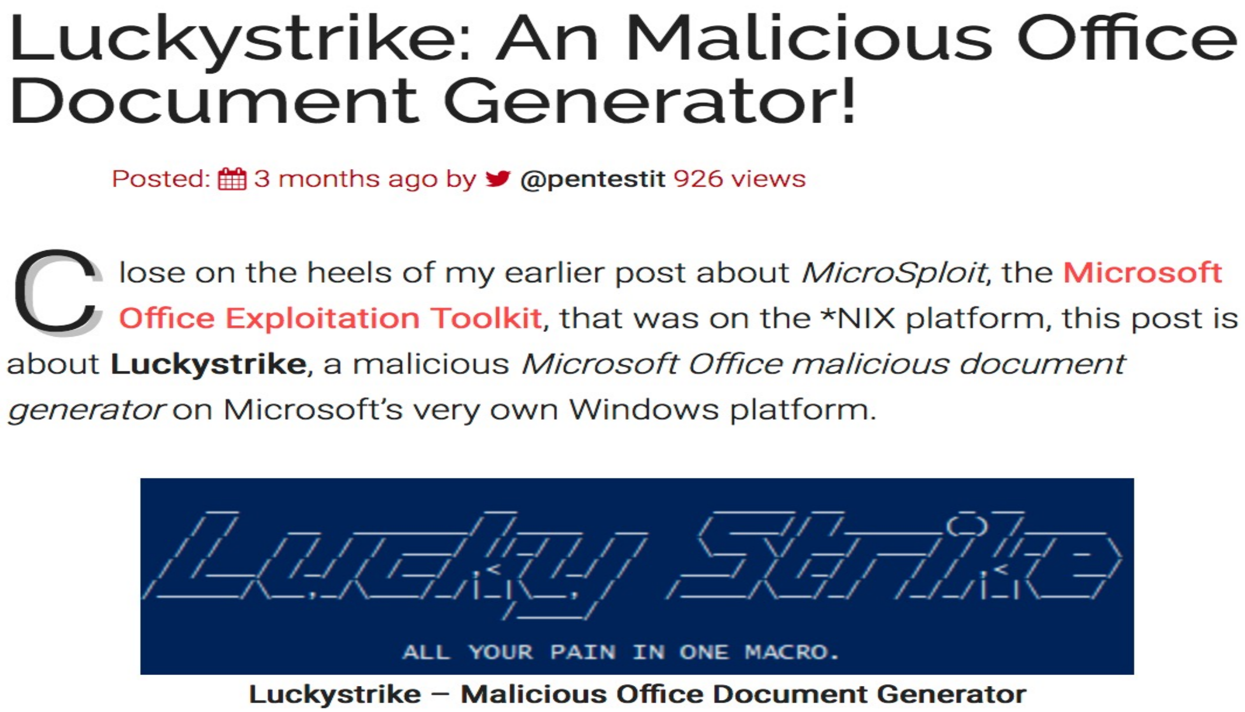
Infrastructure (IOCs)
Methods (TTPs)

Vulnerable

- Any device, system and software is vulnerable
  - 100% perfect doesn’t exist
  - Configuration mistakes (open ports, weak passwords)
  - 0-days, 1-days, multi-days
  - Credentials, credentials, credentials
- Often unpatchable
  - Code not modifiable
  - Vendor intervention required
  - Vendor doesn’t allow patching
- Broad attack surface
  - Office environment + industrial environment
  - Endpoints + servers + network devices + security devices
  - Service providers (MSP, MSS, Cloud, ISP)

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



Luckystrike: An Malicious Office Document Generator!

Posted: 📅 3 months ago by @pentestit 926 views

Close on the heels of my earlier post about *MicroSploit*, the **Microsoft Office Exploitation Toolkit**, that was on the *NIX platform, this post is about **Luckystrike**, a malicious *Microsoft Office malicious document generator* on Microsoft's very own Windows platform.

Luckystrike – Malicious Office Document Generator

Stealthier

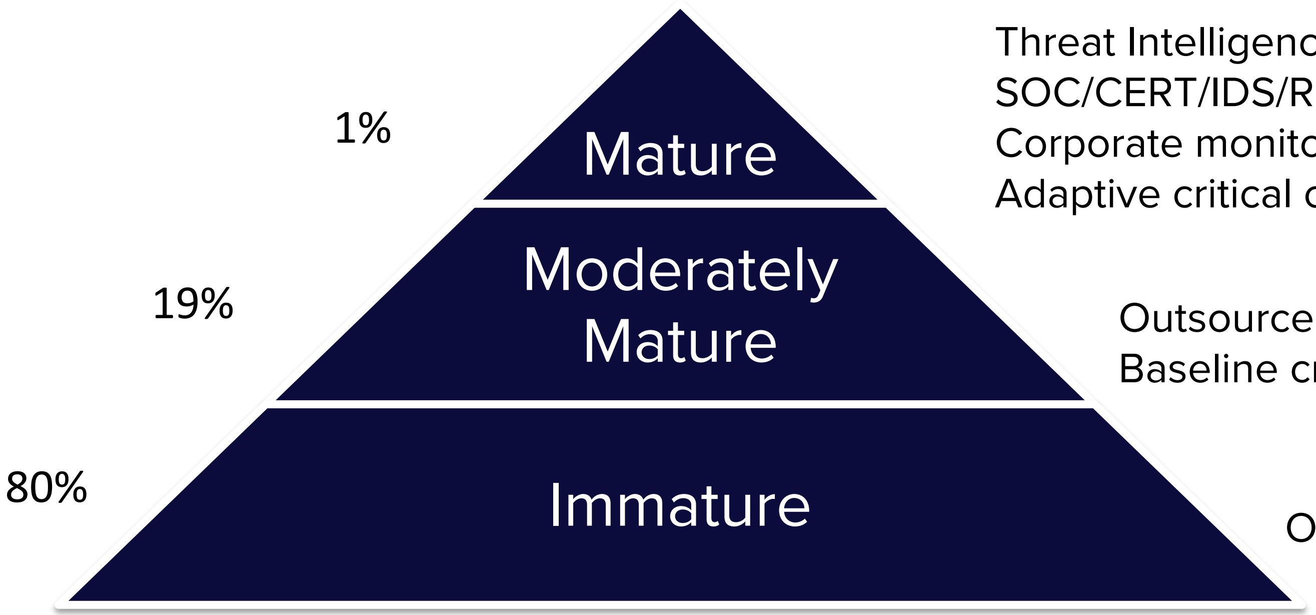
- Masquerading as a trusted origin
- Bypassing protective layers
  - Unpatched vulnerabilities (Flash, Java, MSFT, 0-days)
  - Non-active or low-active content (JavaScript, Macros, PowerShell)
  - Encrypted, password protected, attachments
- Using legitimate OS components (PowerShell, WMI, AMT)
- Using legitimate business credentials

- Prevention becomes more and more difficult

Prevention/Detection

- Critical controls have to adapt dynamically
  - New critical vulnerabilities
  - New methods
- IOCs become less and less useful, maximise their benefit
  - Timeliness and quality
  - Exchange faster and implement automatically
  - Most organisations don’t know how to use them
- TTPs are more stable and valuable
  - No taxonomy
  - No translation in actionable code
- Credentials become critical to monitor

Maturity

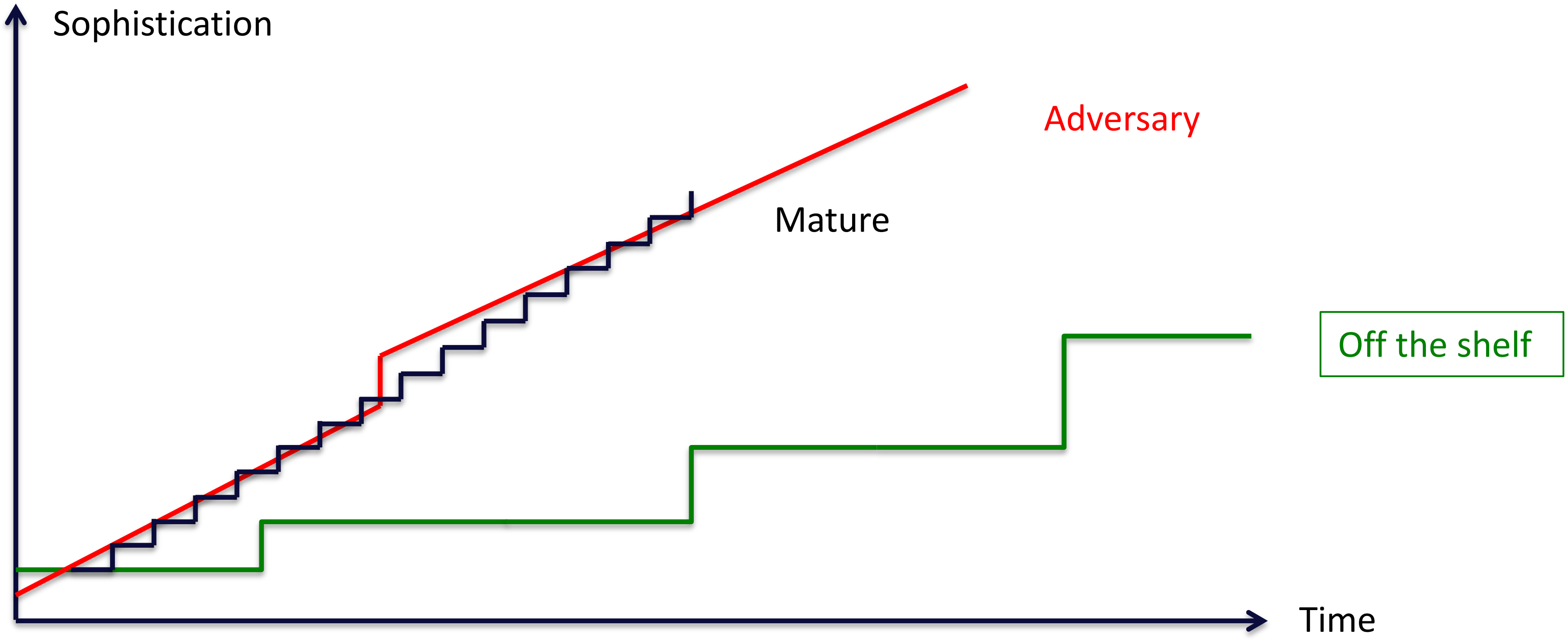


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

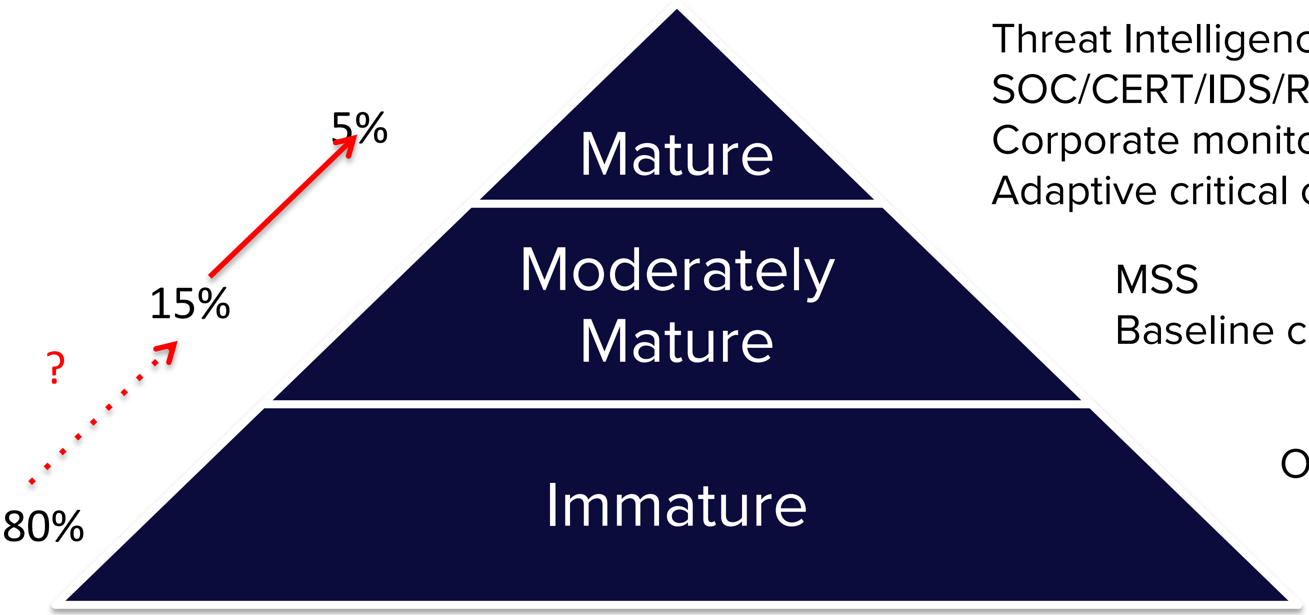
Outsource to MSS
Baseline critical controls

Off the shelf security

Gap



Opportunity

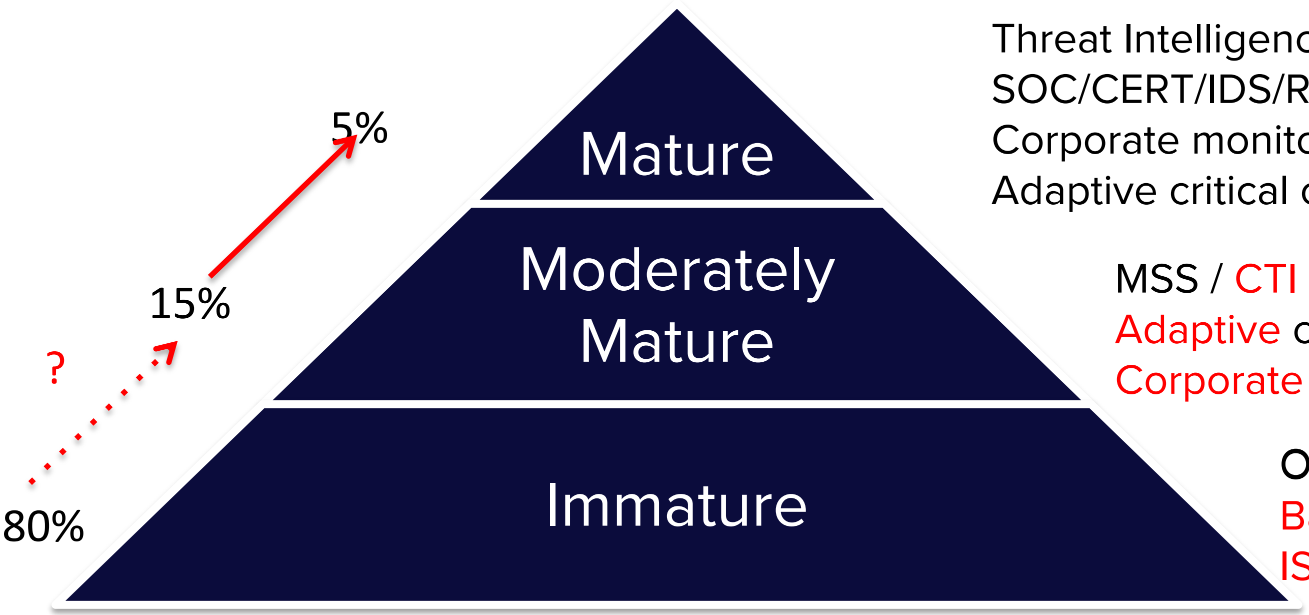


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

MSS
Baseline critical controls

Off the shelf security

Opportunity

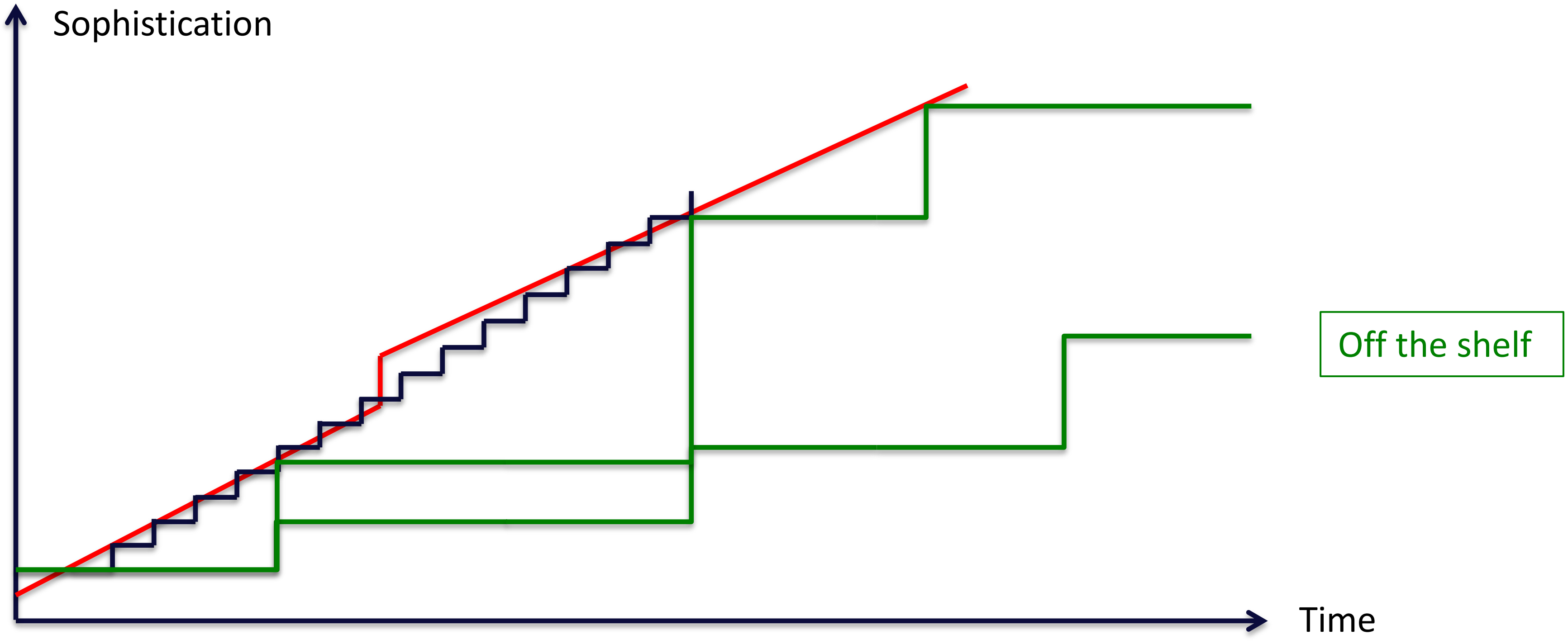


Threat Intelligence / TIP
SOC/CERT/IDS/Red Team
Corporate monitoring
Adaptive critical controls

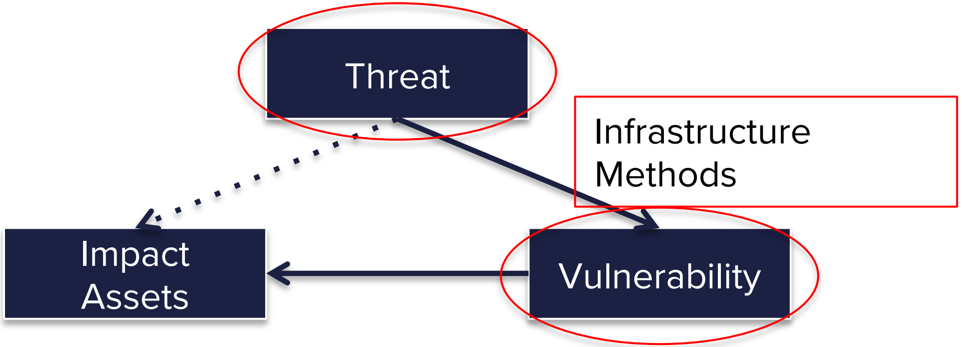
MSS / CTI Fusion Center
Adaptive critical controls
Corporate monitoring

Off the shelf security
Baseline critical controls
ISP protection

Gap



Opportunity



- Community-based
- Adaptive
- Built-in / automated
- Certified

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
- Hunting rules
- Use cases, playbooks, tools
- Adaptive critical controls
- Taxonomies, standards (STIX, TAXII, OpenC2)

Just One More Thing

- Legal impact
  - NIS
  - GDPR
  - E-Privacy
  - CSDR
  - DFS (New York banking law)
  - ...
- Litigation

Target Settlement

- December 2013:
  - 40 mio credit cards stolen
  - 70 mio customers’ private data stolen
- CEO forced to resign
- Class actions and litigation
  - 2015 settlement: $10 million for individual victims
  - 2015 settlement: $67 million with Visa
  - 2015 Settlement: $20 million with MasterCard, rejected
  - 2017 settlement: $18.5 million with 47 states
- Total cost of the breach > $300 million

Take Aways

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

- Raise awareness and train your Management
- Integrate cyber into your normal risk management
- Built-in security for ISP/Cloud
- Strengthen the community
- Offer **real** policy support

- 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