NTA Cyber Threat Intelligence

Staying ahead of emerging threats

About the National Transport Authority

- A statutory non-commercial body
- Established in 2009
- Responsible for developing and implementing strategies to provide high quality, accessible, sustainable transport across Ireland
- NTA funds and oversees Public Service Obligation (PSO) public transport
- NTA is the licensing authority for the commercial bus sector and Small Public Service Vehicles (SPSVs)

What are Emerging Threats

- New vulnerability, with available or easy-to build exploits
- New availability of exploits for a high-risk vulnerability
- Geo-Political Tension (APT nation state threats)
- Alert Logic telemetry showing active attacks against customer base
- Ongoing, large-scale campaign using a few specific exploits or vulnerabilities
- Widespread news coverage of a vulnerability or exploit that is concerning customers
- New wave of ransomware targeting older vulnerabilities

Current & Future Threats

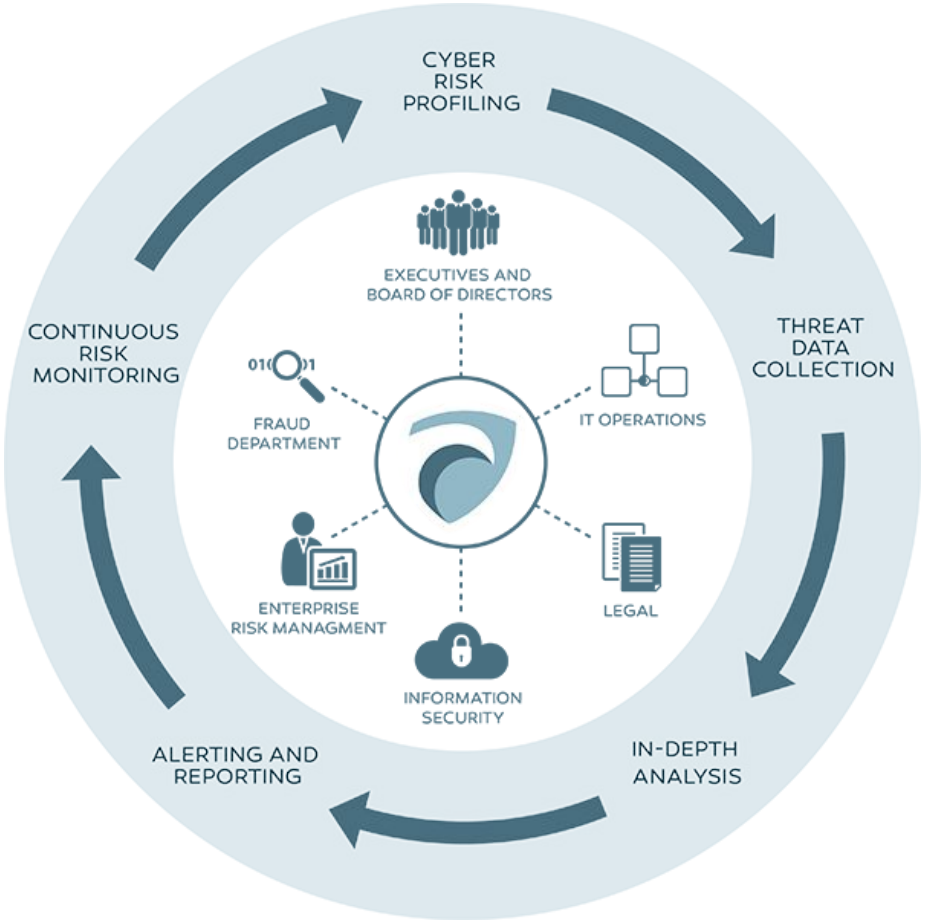
Current:

- APT – Advanced Persistent Threats (State Sponsored)
- Phishing – 99% of malware delivered via Email last 30 days
- Backdoor Attacks – Gaining authorised access to infrastructure and networks
- Hacktivism – Hacktivists aligning to Nation State agendas

Future:

- Phishing will continue to rise significantly
- Delivery of Ransomware to Critical Nation Infrastructure will be targeted
- Operators of Essential Services will see a significant rise in OT & ICS attacks
- Russia, Korea, Saudi, target Government

Staying ahead of Emerging Threats



Cyber Threat Feeds

Staying ahead of emerging threats requires collaboration with our global vendors who detect & mitigate such risks:

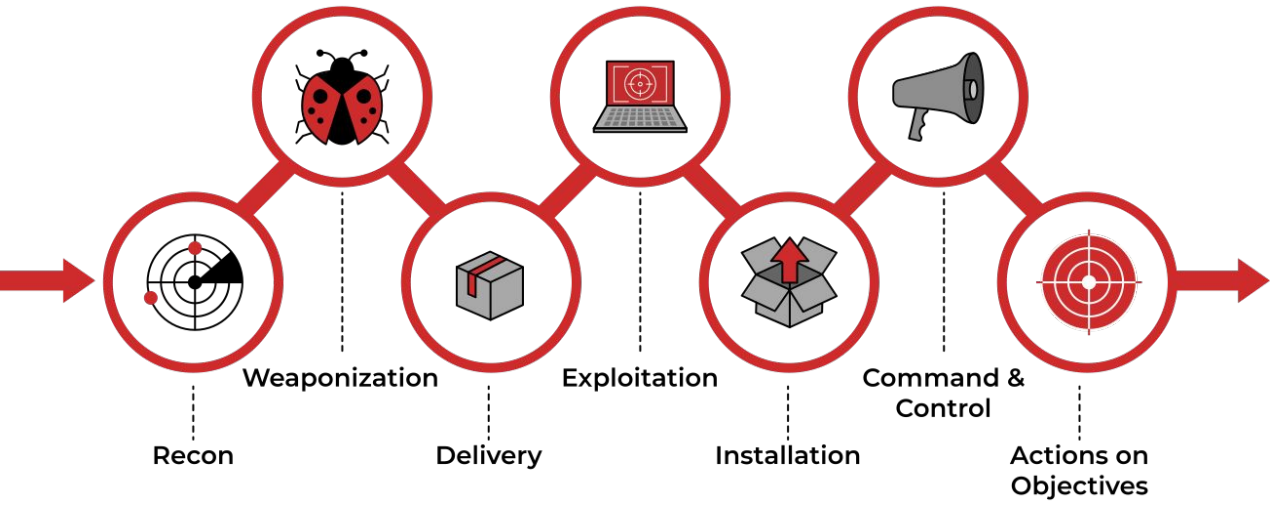
- Mandiant
- Check Point Software Technologies
- Fortinet
- IBM X-Force Exchange

Controls

- Web Application Firewalls & NextGen Firewalls
- Intrusion Detection & Prevention Systems
- Anti Virus & Malware Protection
- Anomalous Behaviour Monitoring
- SIEM Monitoring
- OT Scanning & Monitoring
- Frequent Third & Fourth Party Risk Monitoring

However, That Is Not Enough

Offensive Security



Red Teaming – Offensive Security

Staying ahead of adversary

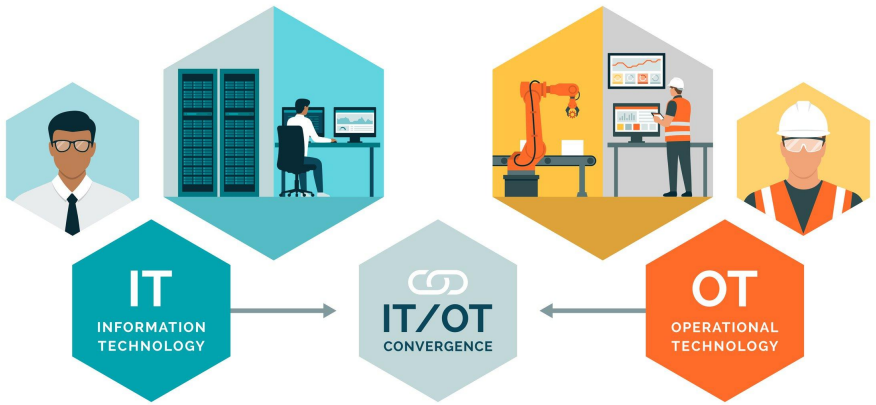
- Dark Web Monitoring
- OSINT (Open Source Intelligence)
- Data Leaks & Credential Leaks (Deep & Dark Web)
- Offensive Security Scanning

Other Activities

- Penetration Testing
- Web Application Scanning
- Port Scanning
- Threat Hunting
- Cyber Threat Intelligence function
- Accidental Insider Threat (Phishing, Stolen Credentials, Malware, Bad Judgement)

Having an effective Cyber Threat Intelligence function, and using all data feeds within your estate, can give you effective information to make informed decisions on your Infrastructure & Network perimeter (Network Segregation, Geo Blocking).

IT, OT & Standards



- A comprehensive guidance on “Securing Operational Technology” has been document by the NCSC which can be found here
- NSCS Cyber Vitals Check List here

Frameworks:

ISO2700X, NIST Cyber Security Framework, PCI DSS/HSM, CSA, CIS & GDPR

Cyber Kill Chain, Mitre Framework,

Cyber Threat Intelligence - Threat Feeds

Web Application & Next Gen Firewalls

- Reactive to threats and attacks
- Insights into attack surface

Intrusion Detection Prevention Systems

- Identifying signatures and malicious attacks /unauthorized access

SIEM, XDR & MDR

- SOC response to alerts and events
- Blue Teaming

Threat Feeds

- Staying ahead of APT with Mandiant, IBM, Fortinet, Check Point, etc etc

Dark Web

- Web Forms
- Chatter
- References

Credential Leaks

- Forms
- Credential Leaks

OSINT

- Open Source Intelligence
- Enumeration
- Discovery & Due Diligence

Architecture

- An Enterprise Architecture approach, Security by Design

End

Questions:

Joe.mccann@intercept.ie