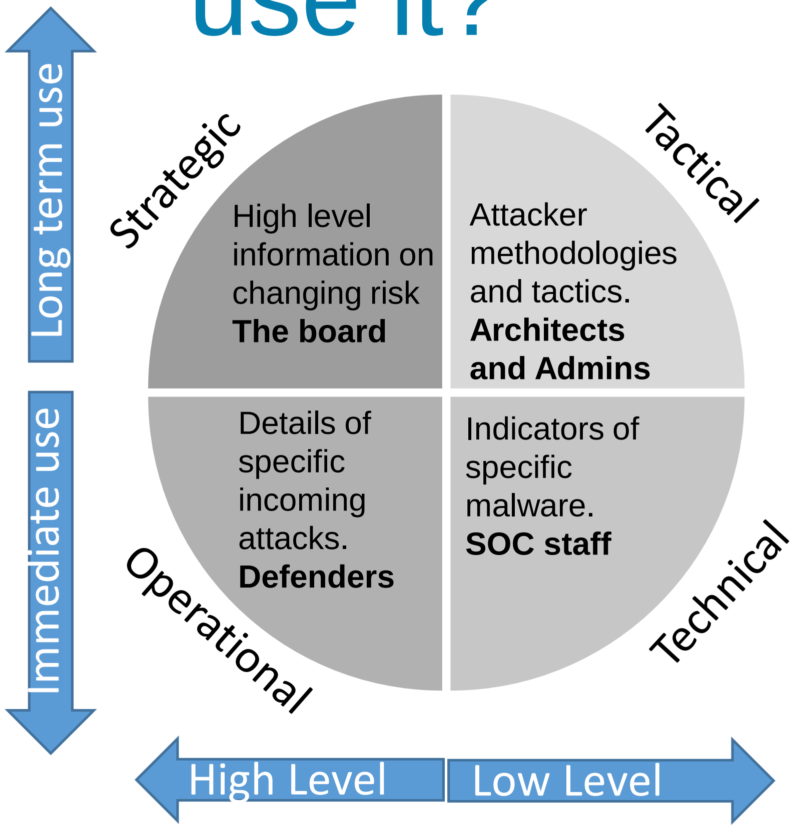
OWASP
AppSec Europe
London 2nd-6th June 2018

Threat Perspectives

From a consulting and a financial services view

Jacky Fox & Gina Dollard

What is Cyber TI and how can you use it?



Long term use

Immediate use

Strategic

High level information on changing risk
The board

Tactical

Attacker methodologies and tactics.
Architects and Admins

Operational

Details of specific incoming attacks.
Defenders

Technical

Indicators of specific malware.
SOC staff

High Level

Low Level

Definition - Threat intelligence is 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 2013

Expectation - Understanding the threat landscape from a dynamic and strategic perspective helps an organisation to prepare for and react appropriately to Cyber events

Some Current Challenges

- TI is poorly understood e.g. threat feeds vs threat intelligence
- Immature partial implementations – a lot are missing information sharing and strategic input
- Application of TI needs a lot of human input we are a long way from fully automated TI
- Security is viewed as an overhead so all initiatives need to have KPIs that show value
- Noise… reaction required? Yes/None/Urgent

Threat perspectives

Operational information & intelligence feeds

STIX™

A structured language for cyber threat intelligence

TAXII™

A transport mechanism for sharing cyber threat intelligence

Internally generated Analysis

- IOC hunters – Darktrace
- End Point Protection
- Security Operation
- Vulnerability Management

Information sharing

- Sectoral – Financial services, public sector
- Geographic – local CERT
- NIS Directive

Generic external

- Open source
- Subscription based - X-Force, Digital Shadows, Deepsight
- Raw e.g. XSS
- Indicators of compromise (IOCs)
- Tactics techniques and procedures TTPs

.

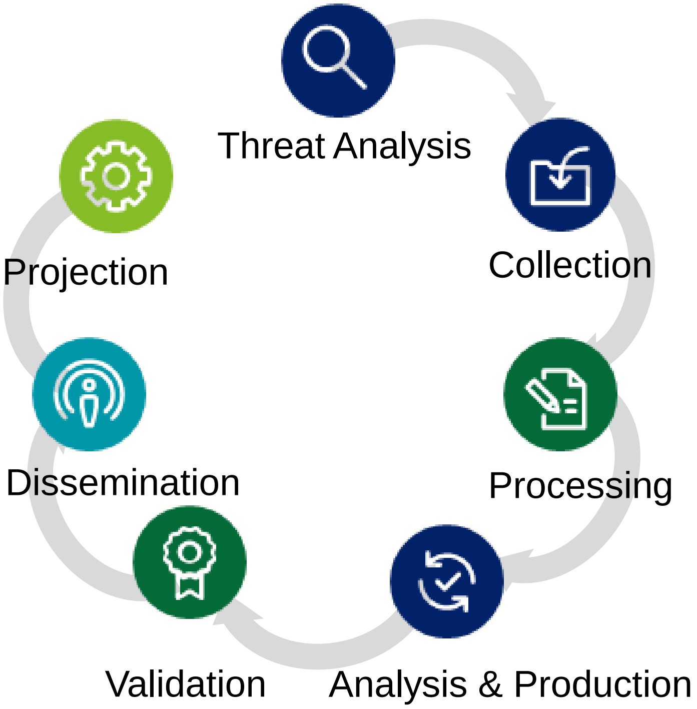
Organisation specific

- Branded “mybank” information
- Social media
- Boards
- Dark web
- Customer or organisation phishing campaigns

Threat perspectives

Use case examples

- Phishing detection
- Incident Response knowledge base
- Vulnerability prioritisation
- Brand monitoring
- Fraud detection



Threat perspectives

Organisation-specific Attack Based Threat Hunting

Hypothetical scenario
Login to a cloud service from a non-corporate device to steal data

Predict and estimate the footprint
Unusual IP/Machine name/OS/Geolocation/time/volume/authorisation failures/upload

Enact or hypothesise and gather artefacts
Inspect logs, ID markers, registry

Block/Alert/Pass?
CEO new phone? Attacker stealing data? Brute force attack?

Learnings
Additional logs, if only we had blocked file downloads from new Geolocations

Produce Custom IOCs

OWASP
AppSec Europe
London 2nd-6th June 2018

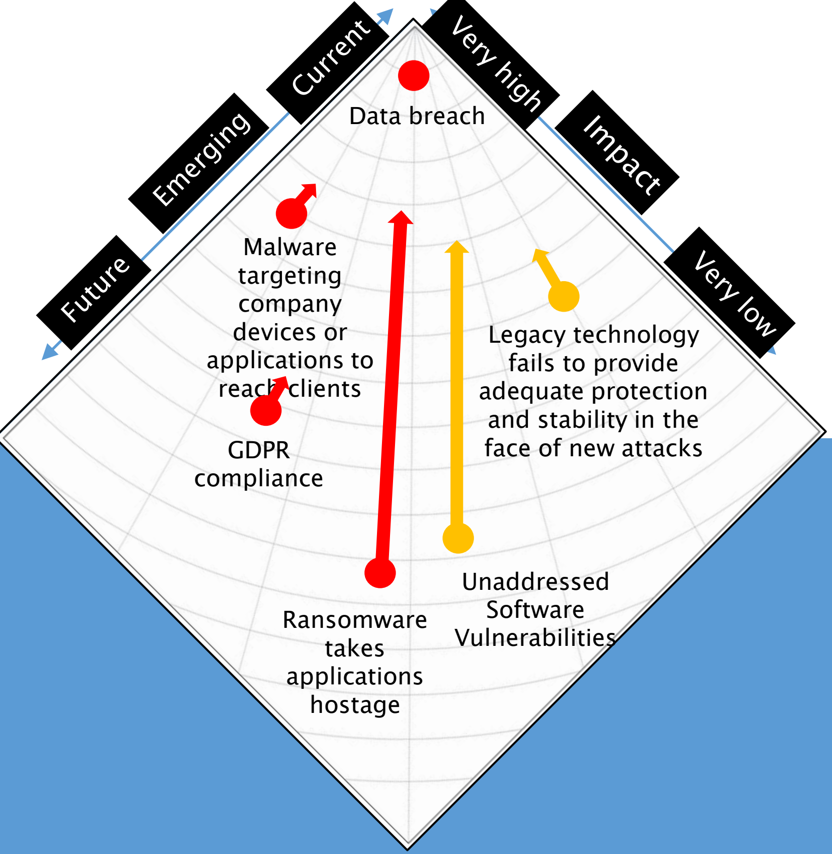
Threat Perspectives

Sources: Deloitte Threat Intelligence & Analysis program

LEVEL OF CONCERN

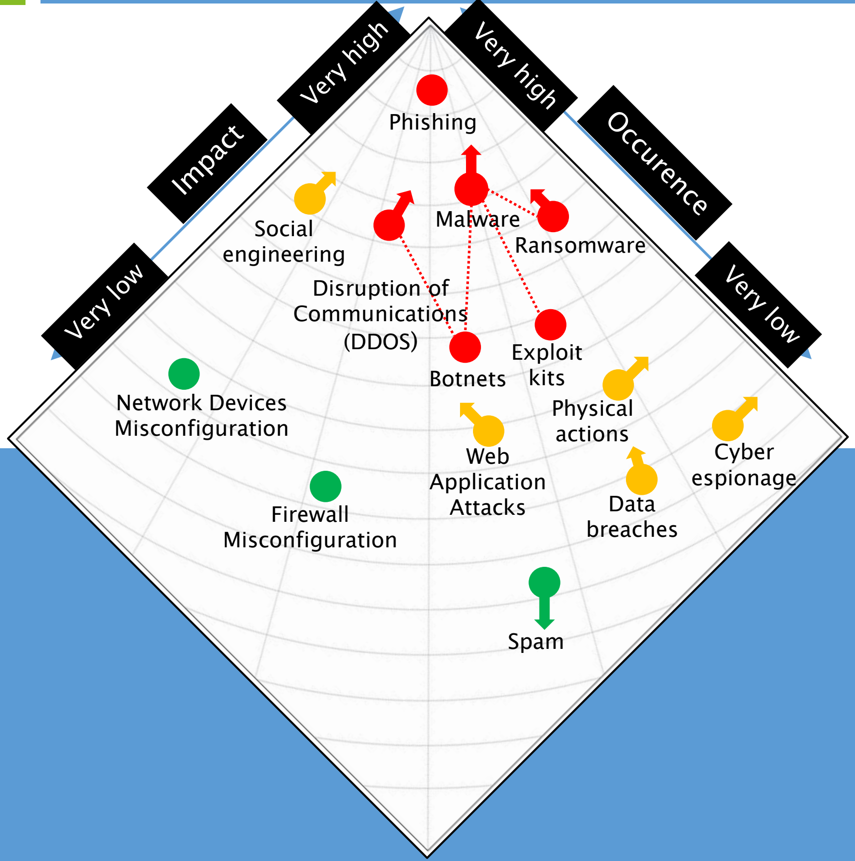
HIGH MED LOW

TOP THREAT SCENARIOS

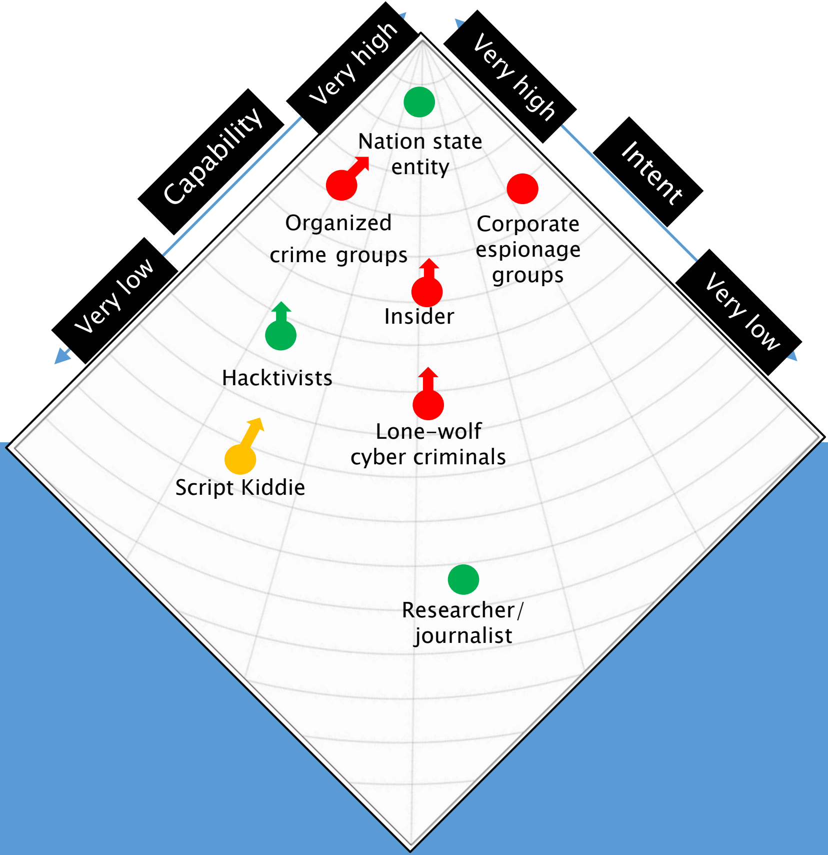


Current
Emerging
Future
Very high
Impact
Very low
Data breach
Malware targeting company devices or applications to reach clients
GDPR compliance
Legacy technology fails to provide adequate protection and stability in the face of new attacks
Ransomware takes applications hostage
Unaddressed Software Vulnerabilities

TOP ATTACK VECTORS



TOP ADVERSARY GROUPS



NOTABLE CYBER SECURITY EVENTS

- Legacy technology is susceptible to attack.
- Ransomware disrupts businesses globally.
- Unaddressed software vulnerabilities can weaken

KEY TAKEAWAYS

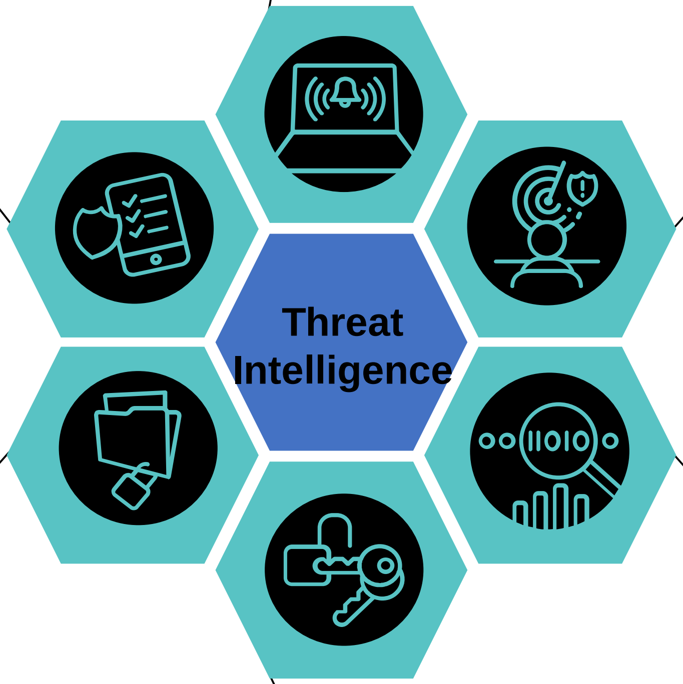
Threat actors develop capabilities and change their attack vectors to take the least difficult approach into your company. For this sector we observed high profile actors targeting for monetary gain, while hacktivism focused on disruption. Tracking industry trends can assist in understanding attack vector changes and form

OWASP
AppSec Europe
London 2nd-6th June 2018

Threat perspectives

Putting some of the pieces together (not exclusive)

Real Threat Intelligence?



IR Playbooks
External, generic and organisation specific playbooks, MITRE framework

Existing RCMs
Control information, risk treatment and residual risk register

Strategic threat analysis
Actors, Vectors and scenarios

Critical Asset register
Value based list of critical assets prioritised to be able to inform threat actions

VM programme
Penetration & vulnerability management data, patch lag information

Operational information
Information feeds, generic IOCs, specific, sectoral, threat hunt IOCs

TIBER-EU

A brief introduction

What is TIBER-EU?

- ECB May 2018
- Threat intelligence based ethical red teaming.
- Production systems
- Identify critical functions e.g. payment services, ATMs
- Mimic tactics, techniques and procedures of real actors insiders or external
- Each regulator can decide to use –EU or to localise TIBER-NL
- Input from tiber-nl (November 2017) & CBEST
- Avoid repeated tests from different bodies via mutual recognition
- Don’t give a pass or fail status – just findings to provide insight and improve posture
- Financial stability of greater EU economy
- Oversight mechanism
- The benefit of cross jurisdictional testing accepted across borders by way of mutual recognition

Who is involved?

- Must be conducted by independent third parties not internal red teams
- A test involves the entity, regulator, external threat intelligence and external red team
- Blue team (who don’t know the test is being conducted)
- White team – internal PM type role

- Financial sector entities definition for TIBER-EU:
- Payment systems, Central Securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and other critical service providers.
- Not limited to financial institutions
- The lead authority decides in any jurisdiction who must or should undertake a test

Threat Perspectives

Preparation phase

- Scope determined and signed off by the board and the regulator
- Critical function identification/confirmation
- Identification of flags
- Qualified Threat Intelligence and Red teams procured? Tender process
- Confidentiality protocols
- Secure document transfer

Threat Perspectives

Risk Management for TIBER-EU?

- Testing on production systems
- Qualifications of TI & RT providers
- Call out of activities that are not allowed during testing e.g. blackmail, bribing, uncontrolled CIA attacks
- Risk and control framework
- Clear escalation procedures and stop button
- Use of code names
- Footprinting risks when mimicking real life attack
- People reconnaissance
- Dark web
- Use of social engineering and under cover

Testing phase

Threats:

- Generic Threat Landscape (TTPs, Actors & Vulnerabilities) – this can be produced by authorities, other agencies or third party, ISACs etc. and updated annually
- General Threat Landscape of national financial sector threat
- Targeted threat intelligence report to incorporate business overview, threat register & recent attacks
- TTI includes attack surfaces, actors & scenarios
- Estimated effort 5 weeks should be broad and deep input using e.g. OSINT and HUMINT

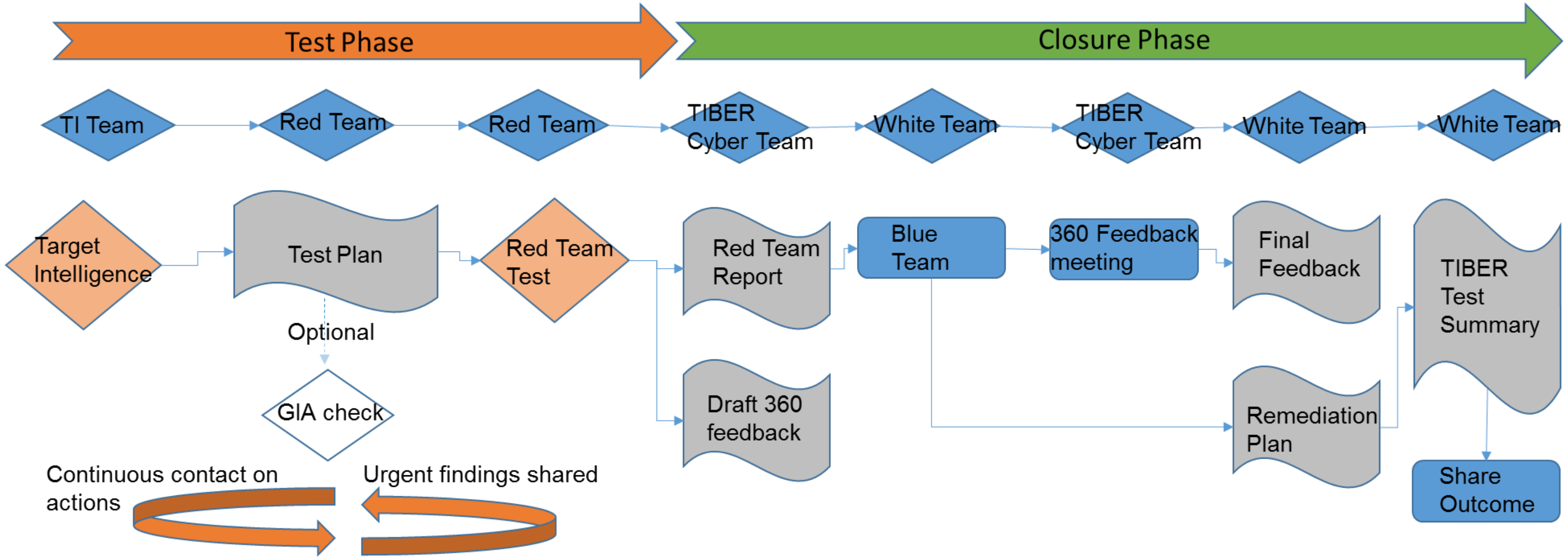
This feeds into

- The red team test plan to inform the chosen flags and targets
- Reconnaissance –use of TI report and other footprinting
- Weaponisation – selection of tools for targets
- Delivery – launch
- Exploitation – actively breaking in,
- Ownership & lateral movement
- Always time limited so if roadblocks are met hints can be given
- Good governance and comms should be in place during the testing

Threat Perspectives

Closure phase

- Red team preliminary test results report
- Blue team are informed of the test and a 360 view is analysed
- Remediation planning controls, policies, education etc. budgets
- Learnings



TI in practice

Gina Dollard

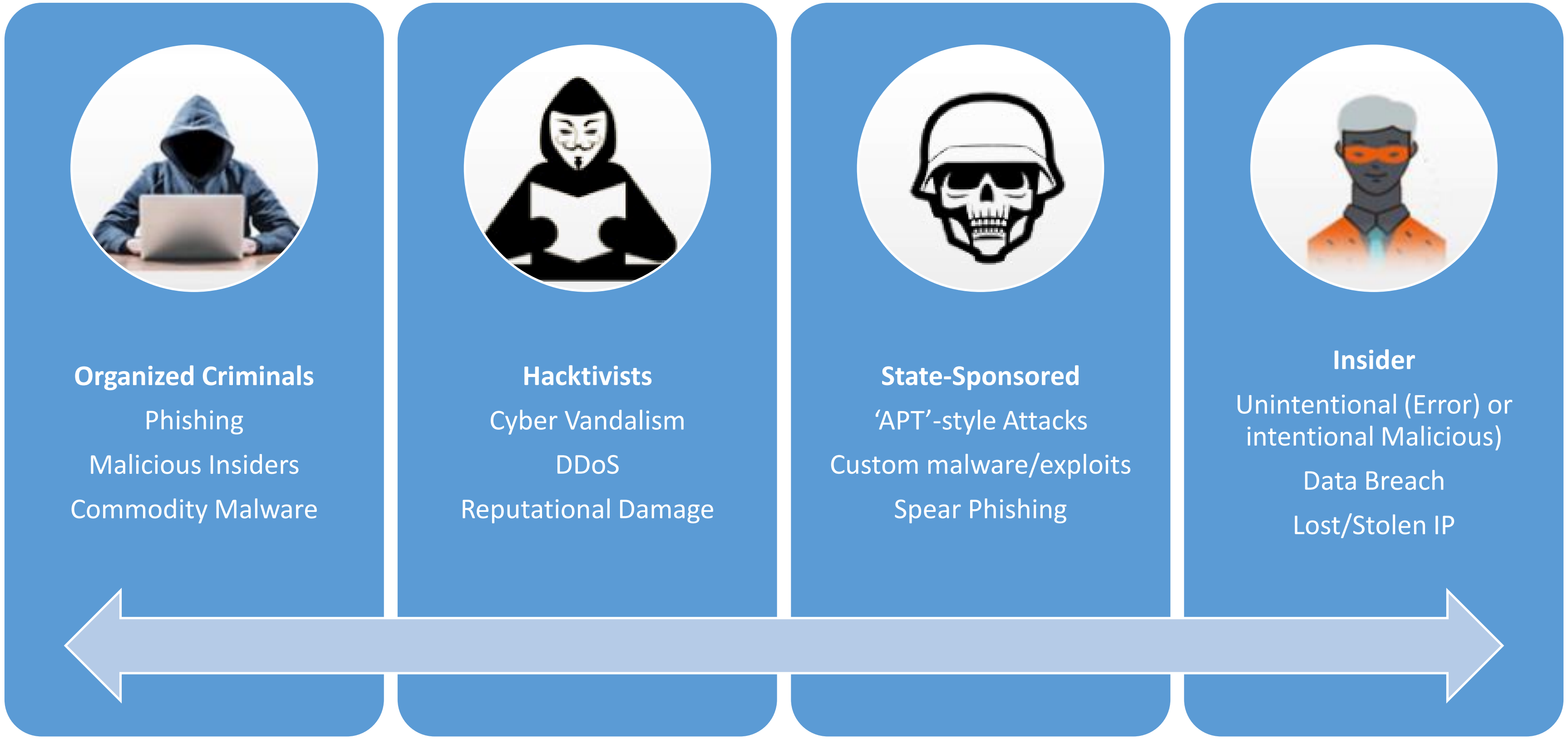
Threat Perspectives

So what does it mean?

TIBER- EU Framework

“Intelligence-led red team tests mimic the **tactics, techniques and procedures** (TTPs) of real-life threat actors who, on the basis of **threat intelligence**, are perceived as posing a genuine threat to entities. An intelligence-led red team tests the use of a variety of techniques to simulate an attack on an entities critical functions (CFs) and underlying systems (i.e. its people, process and technologies). It helps an entity to **assess** its protection, detection and response **capabilities**”

Threat Actor Capabilities



Organized Criminals

Phishing

Malicious Insiders

Commodity Malware

Hacktivists

Cyber Vandalism

DDoS

Reputational Damage

State-Sponsored

‘APT’-style Attacks

Custom malware/exploits

Spear Phishing

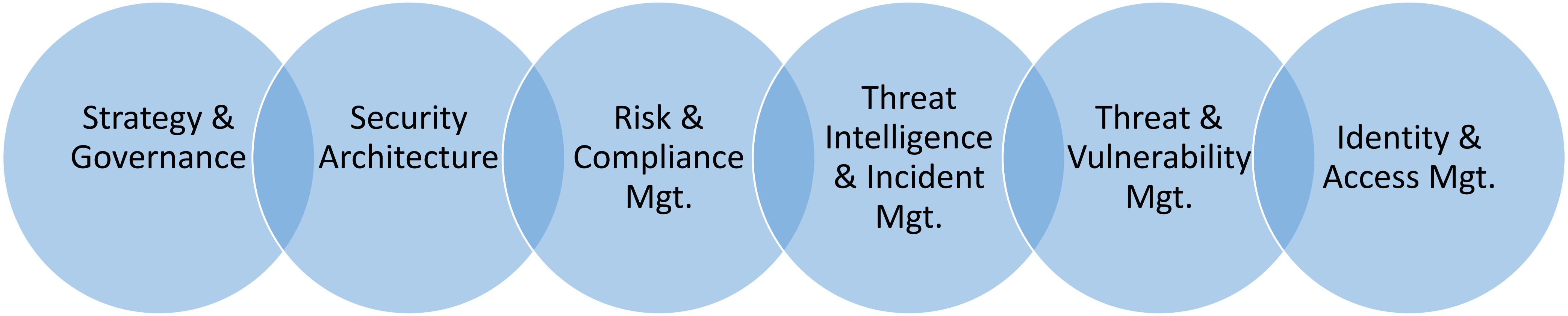
Insider

Unintentional (Error) or intentional Malicious)

Data Breach

Lost/Stolen IP

Security Program



Strategy & Governance

Security Architecture

Risk & Compliance Mgt.

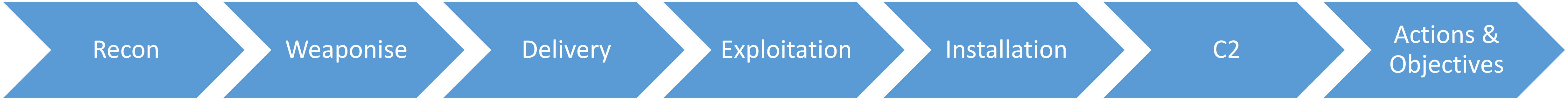
Threat Intelligence & Incident Mgt.

Threat & Vulnerability Mgt.

Identity & Access Mgt.

Kill Chain Analysis

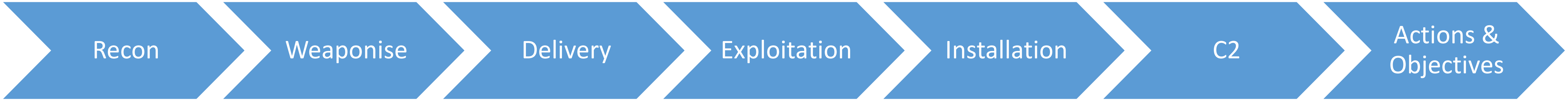
- **Task**: Identify the Attackers’ Step by Step Process
- **Goal**: Disrupting Attackers’ operations



Recon	Weaponise	Delivery	Exploitation	Installation	C2	Actions & Objectives
▪ Motivation ▪ Preparation	▪ Configuration ▪ Packaging	▪ Mechanism of Delivery ▪ Infection Vector	▪ Technical or human? ▪ Applications affected ▪ Method & Characteristics	▪ Persistence ▪ Characteristics of change ▪ Acquiring additional components	▪ Communication between victim & adversary	▪ What the adversary does when they have control of the system

MITRE ATT&CK MATRIX

- ➢ Builds on the Kill Chain
- ➢ Provides deeper level of granularity



Recon

- Motivation
- Preparation

MITRE ATT&CK:
- **Active Scanning**
- **Passive Scanning**
- **Determine Domain and IP Address Space**
- **Analyze Third-Party IT Footprint**

Weaponise

- Configuration
- Packaging

MITRE ATT&CK:
- **Malware**
- **Scripting**
- **Service Execution**

Delivery

- Mechanism of Delivery
- Infection Vector

MITRE ATT&CK:
- **Spearphishing Attachment/Link**
- **Exploit Public-Facing Application**
- **Supply Chain Compromise**

Exploitation

- Technical or human?
- Applications affected
- Method & Characteristics

MITRE ATT&CK:
- **Local Job Scheduling**
- **Scripting**
- **Rundll32**

Installation

- Persistence
- Characteristics of change
- Acquiring additional components

MITRE ATT&CK:
- **Application Shimming**
- **Hooking**
- **Login Items**

C2

- Communication between victim & adversary

MITRE ATT&CK:
- **Data Obfuscation**
- **Domain Fronting**
- **Web Service**

Actions & Objectives

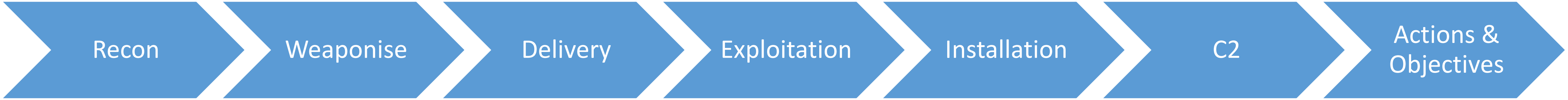
- What the adversary does when they have control of the system

MITRE ATT&CK:
- **Email Collection**
- **Data from Local System/Network Share**

OWASP
AppSec Europe
London 2nd-6th June 2018

Threat Perspectives

Layered Security Controls



Recon

- Motivation
- Preparation

MITRE ATT&CK:
- Active Scanning
- Passive Scanning
- Determine Domain and IP Address Space
- Analyze Third-Party IT Footprint

Security Controls:
- **Policies & Procedures**
- **Firewall**
- **Cyber Awareness Training**

Weaponise

- Configuration
- Packaging

MITRE ATT&CK:
- Malware
- Scripting
- Service Execution

Security Controls:
- **Threat & Vulnerability Mgt.**

Delivery

- Mechanism of Delivery
- Infection Vector

MITRE ATT&CK:
- Spearphishing Attachment/Link
- Exploit Public-Facing Application
- Supply Chain Compromise

Security Controls:
- **Anti-Virus**
- **Web Proxy**
- **Mobile Device Mgt.**
- **Directory Services**

Exploitation

- Technical or human?
- Applications affected
- Method & Characteristics

MITRE ATT&CK:
- Local Job Scheduling
- Scripting
- Rundll32

Security Controls:
- **Anti-Virus**
- **EDR**
- **IDS**

Installation

- Persistence
- Characteristics of change
- Acquiring additional components

MITRE ATT&CK:
- Application Shimming
- Hooking
- Login Items

Security Controls:
- **Anti-Virus**
- **EDR**
- **Policies & Procedures**

C2

- Communication between victim & adversary

MITRE ATT&CK:
- Data Obfuscation
- Domain Fronting
- Web Service

Security Controls:
- **IDS**
- **Web proxy**
- **Firewalls**
- **EDR**

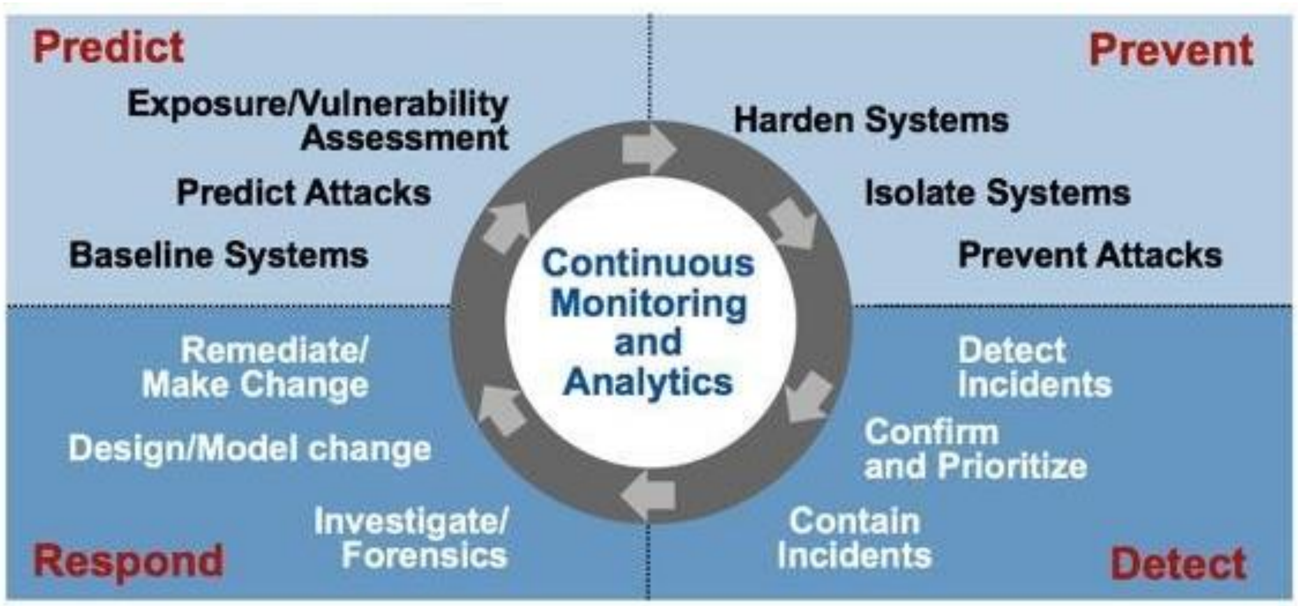
Actions & Objectives

- What the adversary does when they have control of the system

MITRE ATT&CK:
- Email Collection
- Data from Local System/Network Share

Threat Perspectives

Defensive Security Capabilities



Gartner

Threat Perspectives

Intelligence-led Testing

- Should be a nightmare!
- Help identify strengths and weaknesses
- Used to enrich Threat Intelligence

Threat Perspectives

Get Real!

- Informed Stakeholders
  - IT – fit issues,
  - Security Teams – improve capabilities
- Invested Stakeholders
  - Lessons learned
  - Set expectations
  - Advocate for investment

Where to next?

- Automation
  - Improve speed
  - Augment capabilities

- Orchestration
  - Eliminate repetitive, mundane tasks
  - Automate responses
  - Prioritise security events

Getting it Right

Defenders 100%: Attackers 1%