Tackling the Cyber Threat

A Global IT Solution Provider Perspective

Philippe-Emmanuel Maulion

SITA

Create success. Together

WHAT ARE WE GOING TO COVER

- Who is SITA?
- Aviation Transport Industry (ATI) threat landscape
- Cyber Threat Intelligence: Type and Sources
- Applying Threat Intel. to the Attacker Lifecycle
- In Conclusion…

GLOBAL IT SOLUTIONS & SERVICES PROVIDER TO THE ATI

We work with:

- Airlines
- Airports
- Air
- Governments
- Ground Handlers
- Air Traffic Control
- Aerospace
- Travel Distribution

Key facts:

- **400+** Members
- **4,700** staff
- **140** nationalities
- **>60** languages
- **Nearly every** passenger trip relies on our technology and/or services

And we're global

1,000 Airports – presence

>90% The world's airlines

>135 Countries have a SITA presence

WE CONNECT **13,500** air transport industry sites

200 Countries and territories served

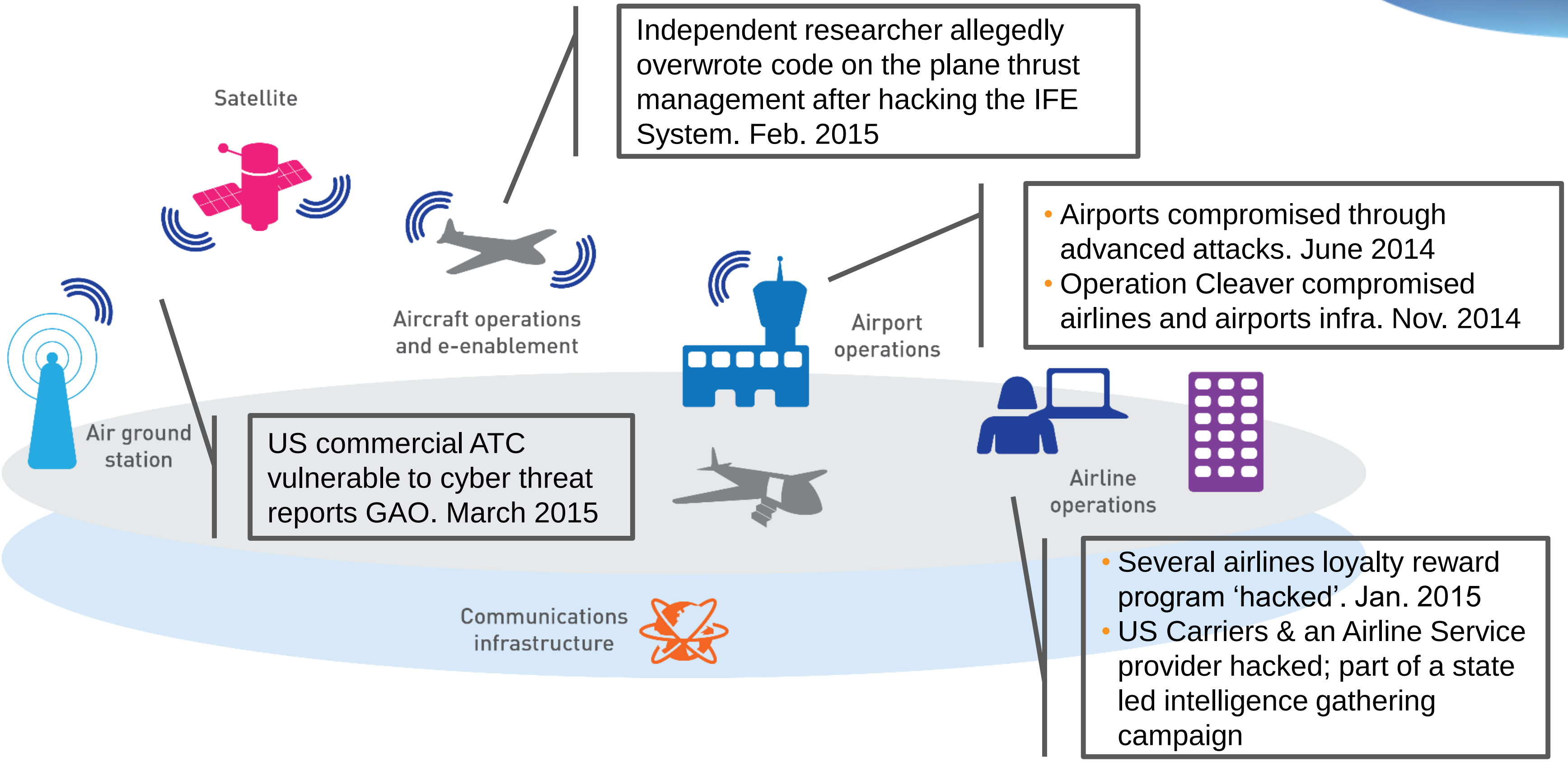
SITA
Create success. Together

THE THREAT LANDSCAPE

Create success. Together

THREAT LANDSCAPE

Aviation is targeted


Satellite
Aircraft operations and e-enablement
Airport operations
Air ground station
Airline operations
Communications infrastructure

Independent researcher allegedly overwrote code on the plane thrust management after hacking the IFE System. Feb. 2015

- Airports compromised through advanced attacks. June 2014
- Operation Cleaver compromised airlines and airports infra. Nov. 2014

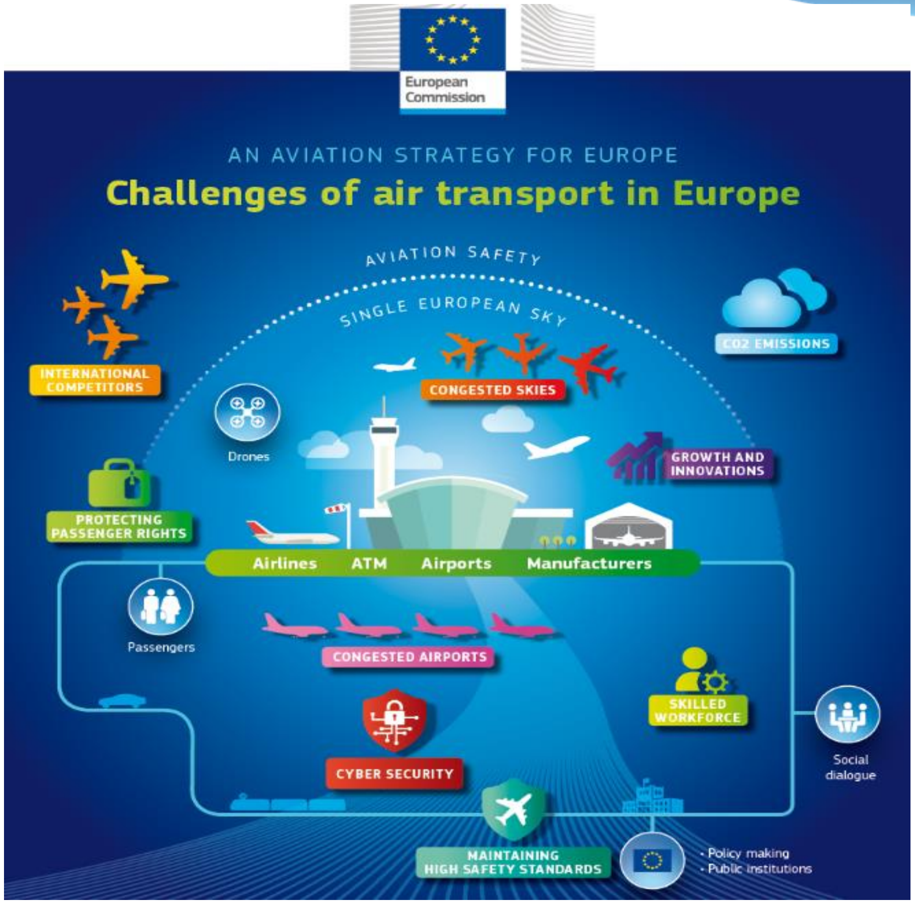
US commercial ATC vulnerable to cyber threat reports GAO. March 2015

- Several airlines loyalty reward program 'hacked'. Jan. 2015
- US Carriers & an Airline Service provider hacked; part of a state led intelligence gathering campaign

➲ Motivated, sophisticated and targeted attacks are evident across the expanse of the global air transport industry

CYBERSECURITY IN THE ATI
A Business Issue

- Sophisticated and targeted attacks are evident across the ATI e.g. Airlines, Aircraft Manufacturers, Airports, etc.
- ‘Aviation and defence firms are likely to remain top targets of cyber espionage activity’ (Mandiant Apr. 16)
- Cybersecurity to remain a Top Management Issue (ACI April 2016)
- Sec. researchers’ work points towards increasingly destructive and disruptive attacks
- Cybersecurity related expenditure forecasted to grow 8.3% CAGR through 2020
- Increase interconnectivity within the industry e.g. e-Aircraft, smart airports, IoT augment risks



RESPONDING TO THE THREAT

Leveraging Cyber Threat Intel. to inform response activities

Create success. Together

ADVERSARIES ARE (SMART) PEOPLE NOT SYSTEMS… THEY PURSUE GOALS

IT'S A "WHO," NOT A "WHAT"

THEY ARE PROFESSIONAL, ORGANIZED & WELL FUNDED

IF YOU KICK THEM OUT THEY WILL RETURN

A HUMAN IS AT A KEYBOARD

HIGHLY TAILORED AND CUSTOMIZED ATTACKS

TARGETED AT THE VICTIM

NATION-STATE SPONSORED

ESCALATE SOPHISTICATION OF TACTICS AS NEEDED

FOCUSED ON ACHIEVING THEIR GOAL

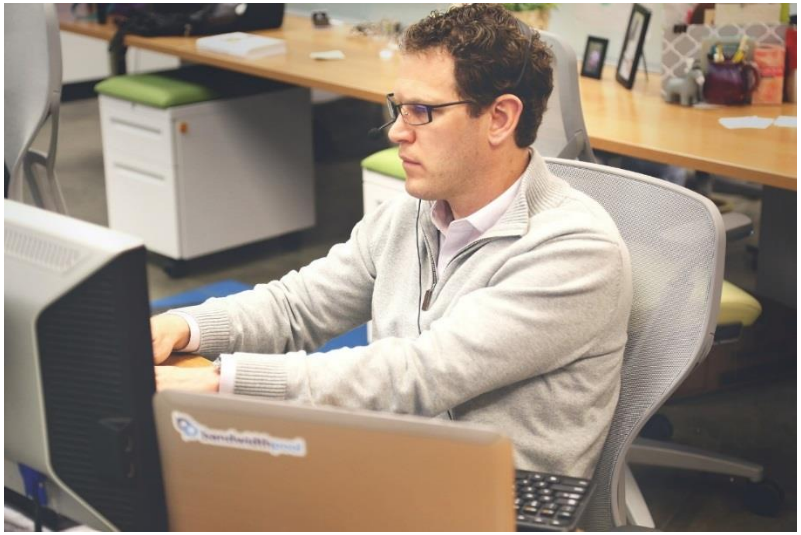
HAVE SPECIFIC OBJECTIVES

AIM AT LONG-TERM OCCUPATION

PERSISTENCE TOOLS ENSURE ONGOING ACCESS

Managing the Threat

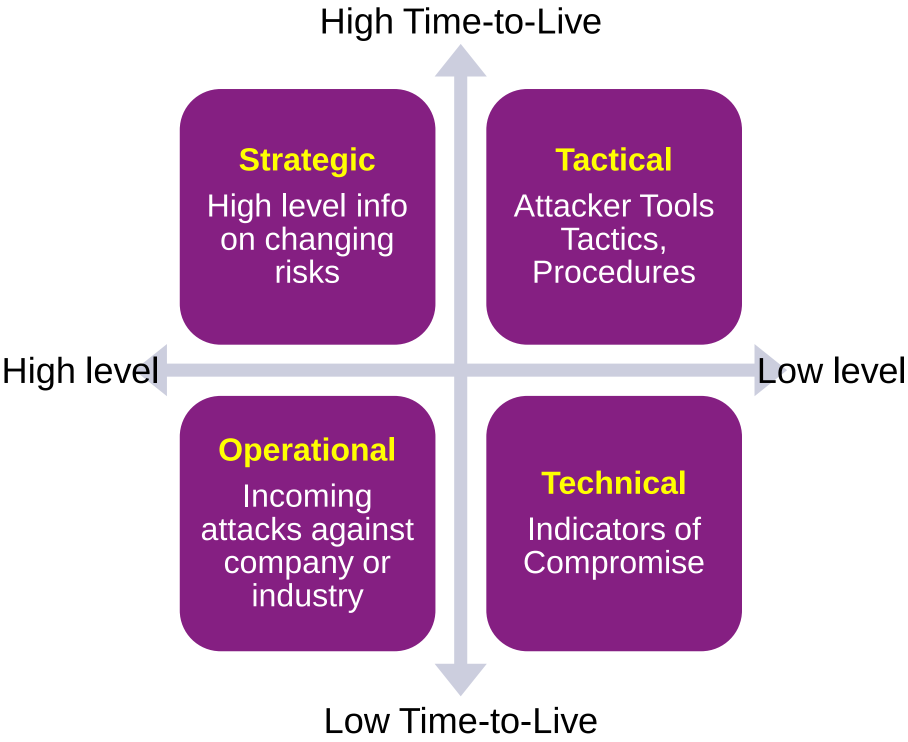
Leverage Threat Intelligence



- Military-style intelligence applied to cyber
- Government-level ‘apparatus’
- Structured
- Years of best practice
- Intelligence reports (mainly) for operational decision making and to inform policy

- Corporate-style IT security approach to threat intel
- Blinky boxes, firewalls, IDS, IR, etc.
- Ad-hoc
- Inventing practice as we go
- Intelligence reports (mainly) for pretty dashboards to management to justify budget

Threat intelligence types and Sources



OSINT Open Source Intelligence

- Derived from open sources (e.g. mainstream media, Internet forums, paste sites, etc.
- **Pros:** good for ‘context’ and ‘big picture’
- **Cons**: multiple languages, interpretation, noise

TECHINT Technical Intelligence

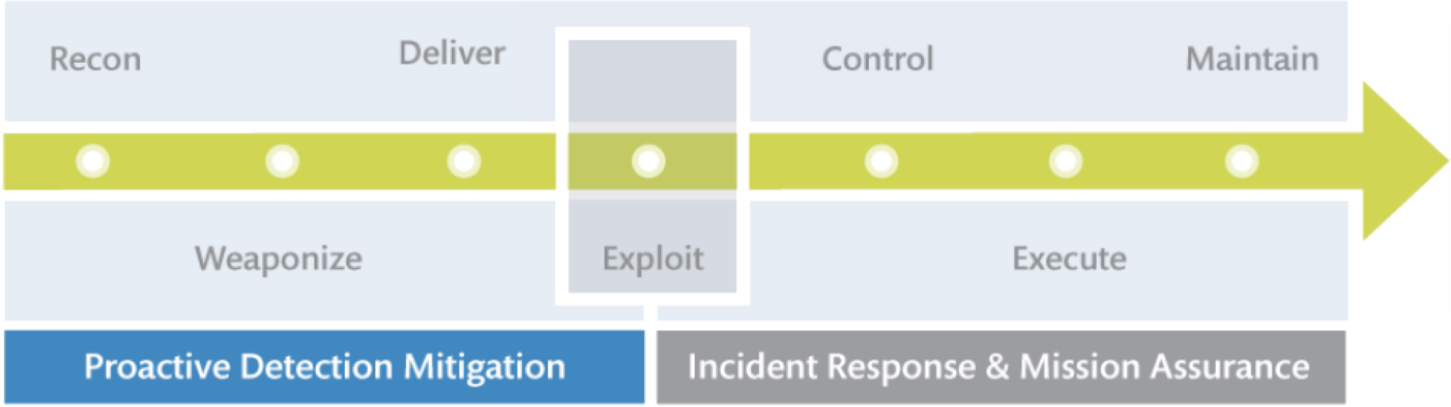
- Technical indicators (e.g. IP addresses, hashes, domains, tools & techniques)
- **Pros:** easy to consume and drive automation
- **Cons:** difficult to ‘contextualize’

SIGINT Signals Intelligence

- Derived from analysis of communications, often in one’s own environment
- **Pros:** low noise; if you’re seeing it, you’re experiencing it
- **Cons:** requires extensive apparatus

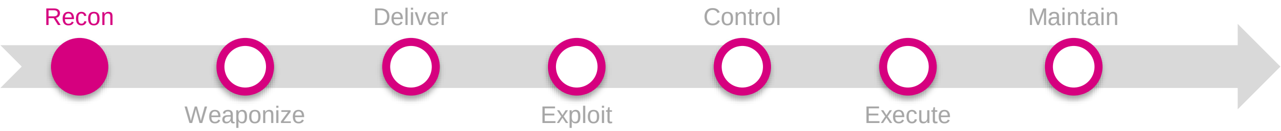
Cyberattack lifecycle

- Describes the stages that an adversary must go through in order to realize their goals against their target(s).
- From defender’s point of view, represents the many ways we can disrupt the adversary


Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Proactive Detection Mitigation
Incident Response & Mission Assurance

The MITRE Corporate Cyber Attack Lifecycle

SITA
Create success. Together



OSINT

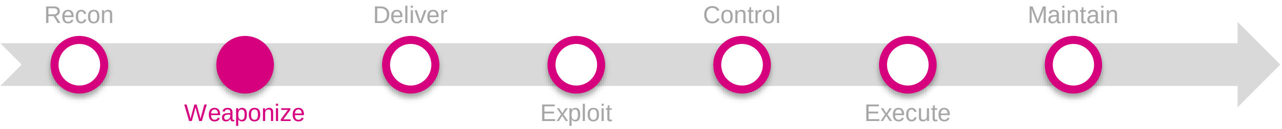
- Paste sites and underground forums can be rich sources of information
- Perform your own reconnaissance… what can you find about **you**?

TECHINT

- IP addresses of adversary command-and-control infrastructures
- E-mail addresses of targeted staff members
- Your own external footprint... what's out there vs. what we *thought* was out there?
- Proactively look for vulnerabilities and technical weaknesses

APPLICATIONS

- Target lists of IP addresses, domain names, email addresses, etc. to feed monitoring
- Discover 'rogue' or 'shadow IT' services to determine where security monitoring / response coverage gaps might exist



Recon

Weaponize

Deliver

Exploit

Control

Execute

Maintain

OSINT

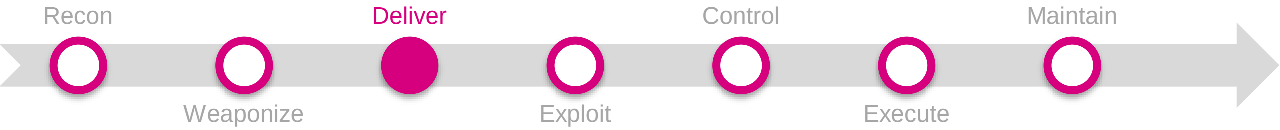
- Attacker’s tools, techniques and procedures (TTPs) may have been reported (semi) publicly
- Security researchers posting proof-of-concept code
- Adversaries sometimes let their code slip!

TECHINT

- Many attacks leverage known tools… so why not acquire them?
- What fingerprints can identify a tool, or technique?

APPLICATIONS

- Download attacker tools: maybe work with your pentesting team and build detections for common tools (e.g. mimikatz, PowerShell Empire, etc.)
- Proof-of-concept code can help highlight where vulnerability exists… can inform business proactively of need to be vigilant



OSINT

- Research delivery mechanisms
- Malware reports, reverse engineering write-ups, etc.

TECHINT

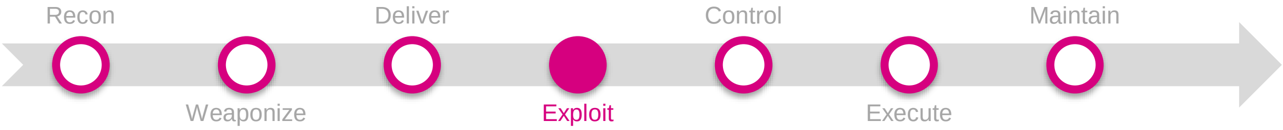
- Malware signatures, hashes
- IP addresses of delivery mechanisms

SIGINT

- Monitor incoming email
- Enable a reporting mechanism for staff to report malicious email

APPLICATIONS

- Ingest high-confidence intel into defensive controls, like firewalls, IDS/IPS, etc.
- Tune email infrastructure to detect/block known delivery mechanisms



Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain

TECHINT

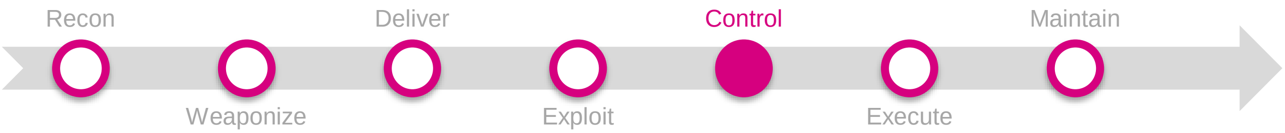
- Attacker TTPs
- Malware signatures
- Exploitation fingerprints (e.g. file/registry artifacts, etc.)

SIGINT

- AV detections
- IDS detections
- SIEM / other monitoring detections

APPLICATIONS

- Malware signatures may enable ‘hunting’ for other infected systems
- Can initiate Incident Response with information about where to start looking
- Assist in helping to ‘scope’ the incident



TECHINT

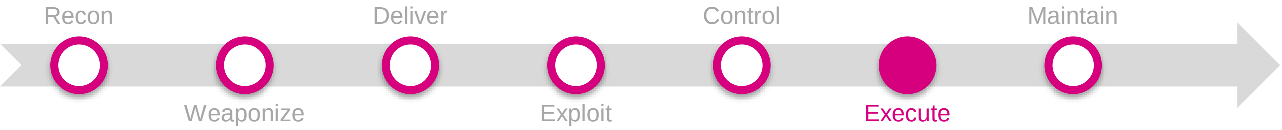
- IP addresses of command-and-control
- C2 domains
- C2 communications protocol details

SIGINT

- Outbound communication to C2 (e.g. beaconing)

APPLICATIONS

- Create detections for certain C2 traffic patterns
- Potentially ‘spy’ on C2 traffic to understand what attackers activity is
- Possible use for blocking & tackling; disrupt C2?
- Further identify scope of a potential incursion



Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain

OSINT

- Attacker data dumps – aka ‘loot’
- Attempts to sell or fence data (cash out)
- Boasting & bragging

TECHINT

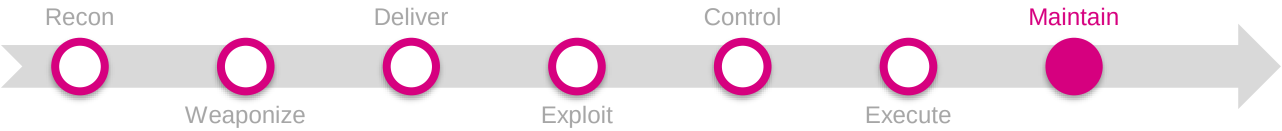
- Details of exfiltration methods
- Forensic artifacts

SIGINT

- Attacker ‘fingerprints’
- C2 and exfiltration communications

APPLICATIONS

- Credentials of compromised users – can alert and take action (e.g. password reset)
- Clearer view of what extent of compromise may be (e.g. data accessed or modified)
- Input to ‘remediation activities’ to block the attacker



OSINT

- Uncover persistence mechanisms and approaches (through research)
- Identify C2 infrastructure

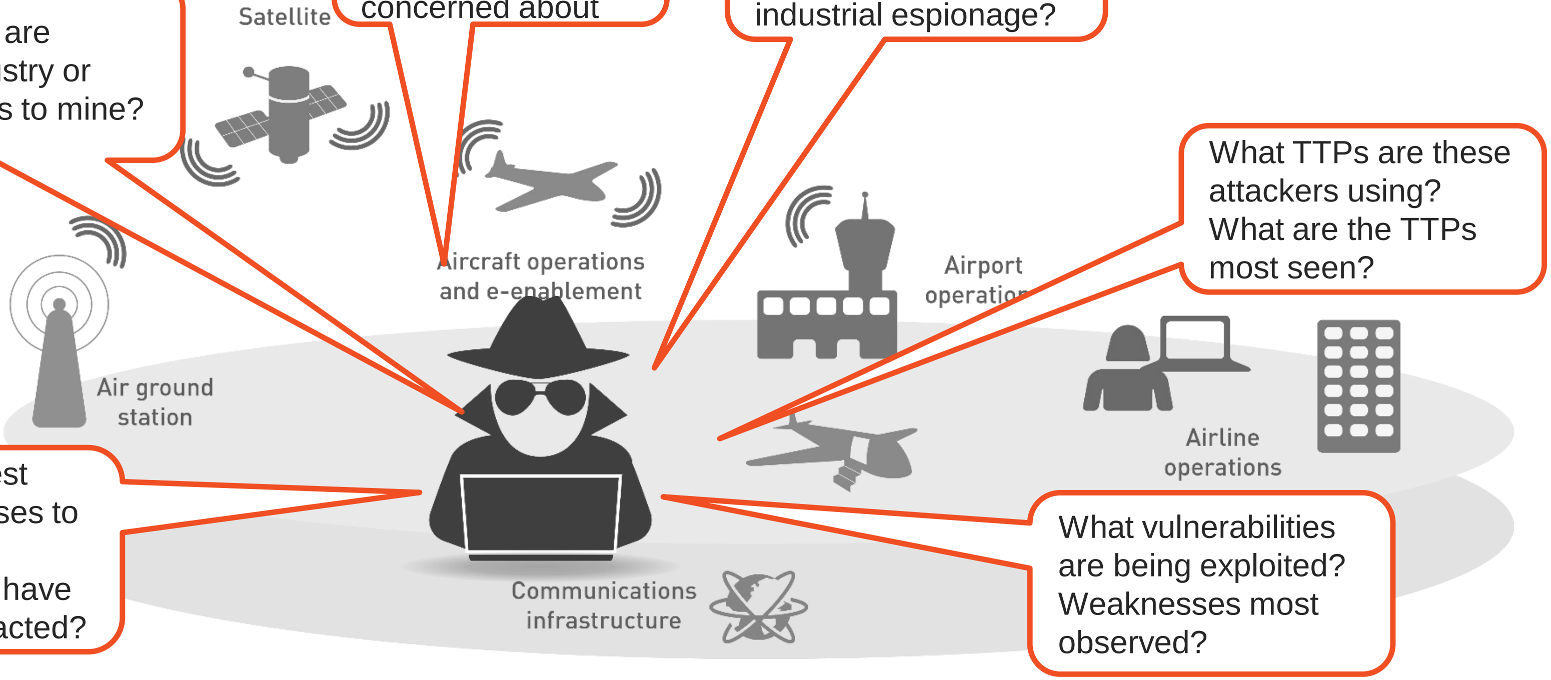
SIGINT

- Compare activity against baseline ‘normal’
- Use of common tools, by uncommon users of those tools (e.g. psexec, PowerShell, etc.)

APPLICATION

- Pinpoint ‘hotspots’ to investigate for signs of malicious activity
- Round-out identification of all access mechanisms ready for remediation

CYBER THREAT INTELLIGENCE


Satellite
Aircraft operations and e-enablement
Airport operations
Air ground station
Airline operations
Communications infrastructure

What campaigns are targeting my industry or similar companies to mine?

Who are the adversaries I should be (most) concerned about

What is the nature of the attacker e.g. criminal, hacktivism, industrial espionage?

What TTPs are these attackers using? What are the TTPs most seen?

How should I best adapt my defenses to counter these attackers? How have other victims reacted?

What vulnerabilities are being exploited? Weaknesses most observed?

Overarching goals:

- support informed decision making; clarify the risk landscape
- prevent or decrease the time to detect an attack
- augment incident response capability; facilitate investigation of an attack
- improve information security management practices

3 points in conclusion

1

The **cybersecurity threat** is real, co-ordinated and **happening now** – across all industries

2

Cybersecurity intelligence can help individual organisations address and respond to threats,

3

Industry**-wide shared intelligence is most helpful** to protect our industry

Get involved… share your cyber threat intelligence

SITA

Create success. Together

Create success. Together

Create success. Together