FIREEYE™ | MANDIANT®

Cyber Security Resilience

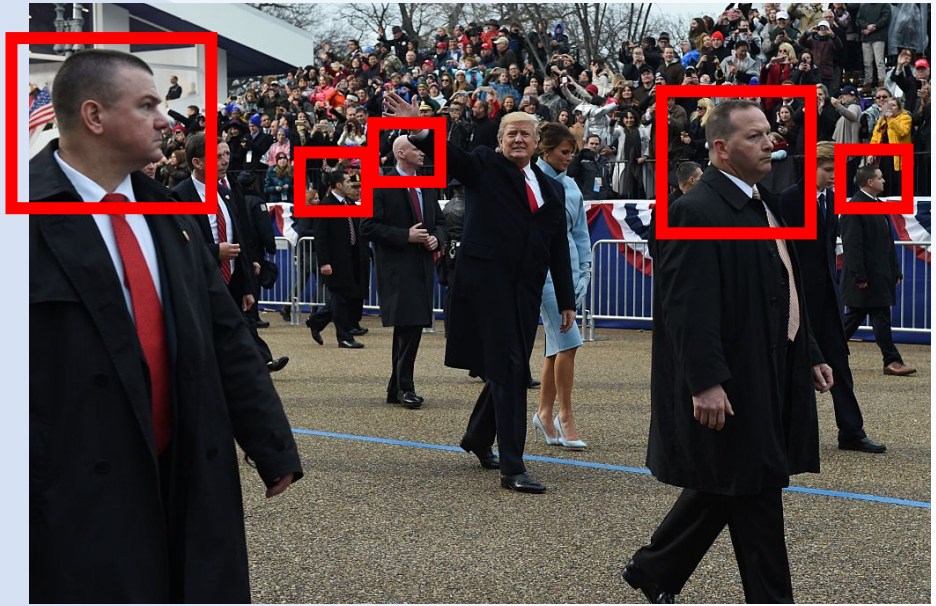
Gabriele Zanoni - Mandiant

Executives are more focused on cyber resilience

- Are critical digital assets protected?
- Are we susceptible to the attack that just happened to company X?
- Can we minimize the impact of a Ransomware attack?
- Could actor group (XYZ) compromise us?
- Can we be compromised by a malicious insider or accidental loss?

Can you provide quantifiable evidence of cyber resilience?

Let's start from the real life



Where are they looking?

Learning from the Secret Services

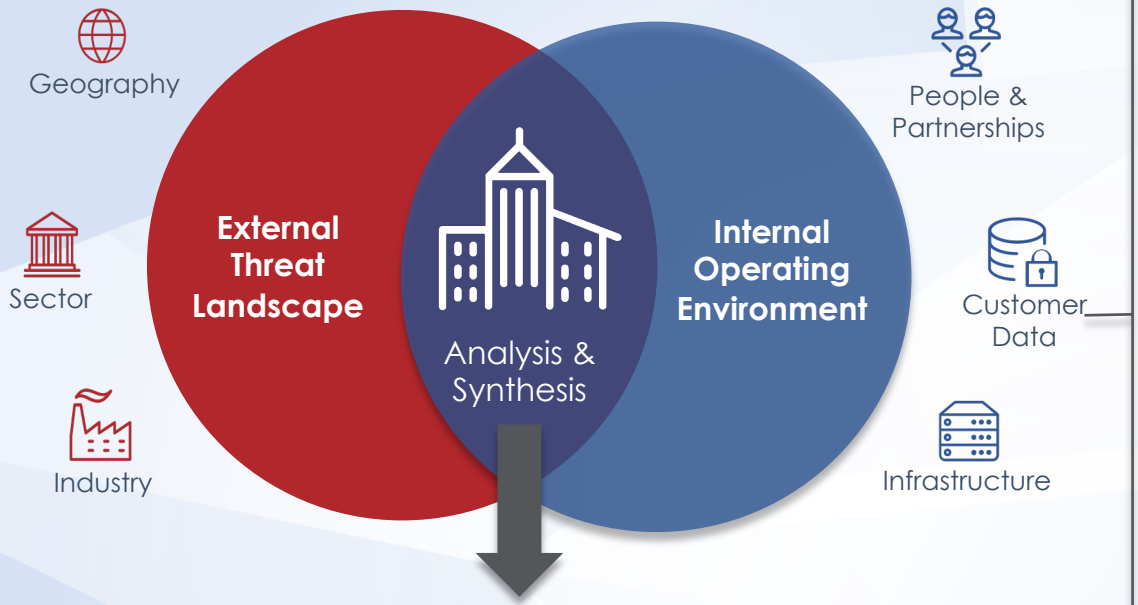
- They are NOT checking if today the President has or not a bulletproof vest.
- They are looking at people on the rooftops, vechicles approacing, they look for hands stuffed in pockets and other signs of suspicious activity. And they wear sunglasses so that they scan the crowd without tipping off any potential suspects.

In summary:

- They are **NOT looking at the Vulnerabilties.**
- They **are looking at the Threats.**

Can you do the same for the CyberSpace?

Developing a Cyber Threat Profile



External threat landscape knowledge, coupled with a **clear understanding** of your **current security posture** and your ability to **anticipate, mitigate and respond** are key to success.

A Tailored Threat Profile should:

Outline the **relevant threats** you need to **prepare for**

Incorporate **evidence-based analysis techniques** to drive **threat prioritization**

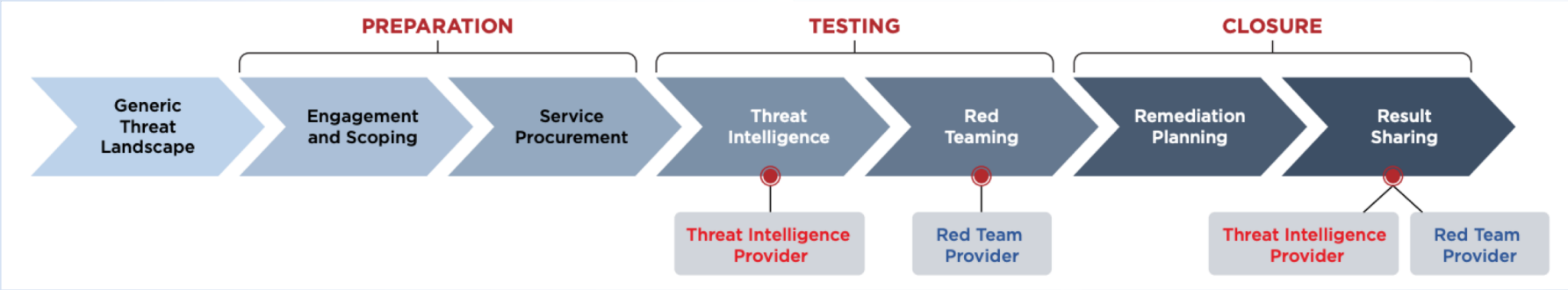
Capture **key business services, critical infrastructure, operating environment** knowledge

Provide **inputs to leadership, cyber defense & risk functions**

Be a **core intelligence product** that is **updated at regular intervals** (i.e. every 6mths or annually)

Cyber Resilience for Financial Institutions with TIBER-EU

- The Threat Intelligence Based Ethical Red Teaming (TIBER) EU is a framework published by the European Central Bank for delivering "a controlled, bespoke, intelligence-led red team test of entities' critical live production systems."
- **Threat Intelligence** provider collects, analyses, and disseminate intelligence from other sources about relevant threat actors and probable threat scenarios for the institution.
- **Red Team** provider will execute an intelligence-led test of specified critical live production systems, people and processes that underpin the institution's critical functions.



Discover where your risk exposure is higher

- Security posture might vary after a Merge and Acquisition activity.
- Need to ensure consistency in the security levels and zones.
- Where I need to focus?

Response Readiness Assessment

Asses and technically validate your cyber defense capability against Mandiant's six core response readiness competencies through a combination of:

- Documentation review,
- Analysis of logging configurations,
- Deep-dive workshops,
- Tabletop exercises and
- Simulated testing of your threat detection and prevention controls.
- Threat Detection Controls Testing

Eliminate uncertainty about your response readiness by evaluating your ability to manage threats most relevant to your organization and become cyber-resilient.

Gain guidance, including detailed, prioritized recommendations and an improvement roadmap, to help you realize practical and meaningful improvements for your cyber resilience capability.

Thanks

gabriele.zanoni@mandiant.com