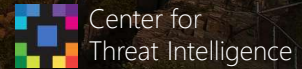


Threat Intelligence: Anticipating and Preventing Attacks Before They Happen... Here's How!

Janet Lawless
CEO/Founder
Center for Threat Intelligence

jlawless@centerforti.com
www.centerforti.com



www.CenterforTI.com

Confidential

©2023 Center for Threat Intelligence

1



Center for Threat Intelligence



Enterprise Intelligence Services

- Threat Intelligence Program Development
- Strategy Development
- Insider Threat Program Development
- Intelligence Assessments
- Customized Consulting

Certification

Certified Threat Intelligence Specialist (CTIS)

Professional Development

- Behavioral Psychology of the Insider Threat
- Creating the enemy within: Deconstructing adversary's tactics and strategies to infiltrate your organization
- Mindset and Bias
- Intelligence Training
- Critical Thinking
- And much, much more...

Approved provider for the U.S. Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS).

www.CenterforTI.com

Center for Threat Intelligence ©2023



2

Key Take Aways



www.CenterforTI.com

Center for Threat Intelligence ©2023



3



www.CenterforTI.com

Center for Threat Intelligence ©2023



4

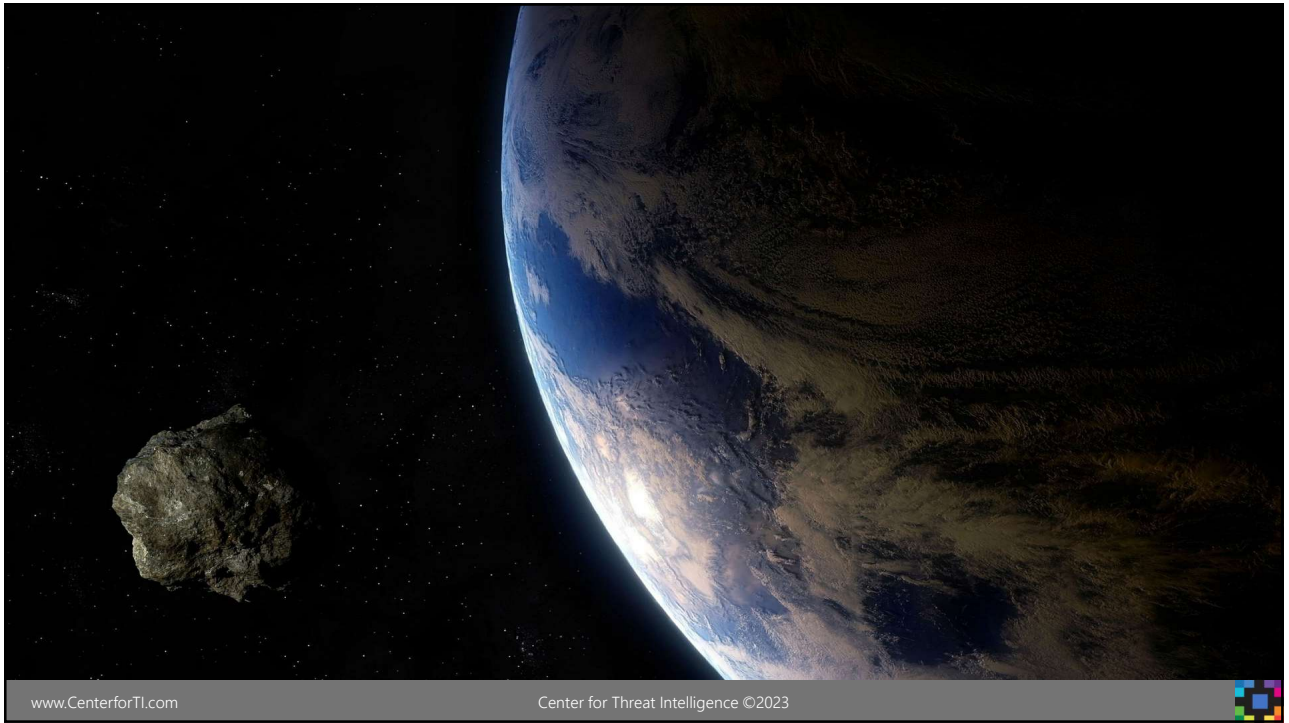


www.CenterforTI.com

Center for Threat Intelligence ©2023



5



www.CenterforTI.com

Center for Threat Intelligence ©2023



6



7



8

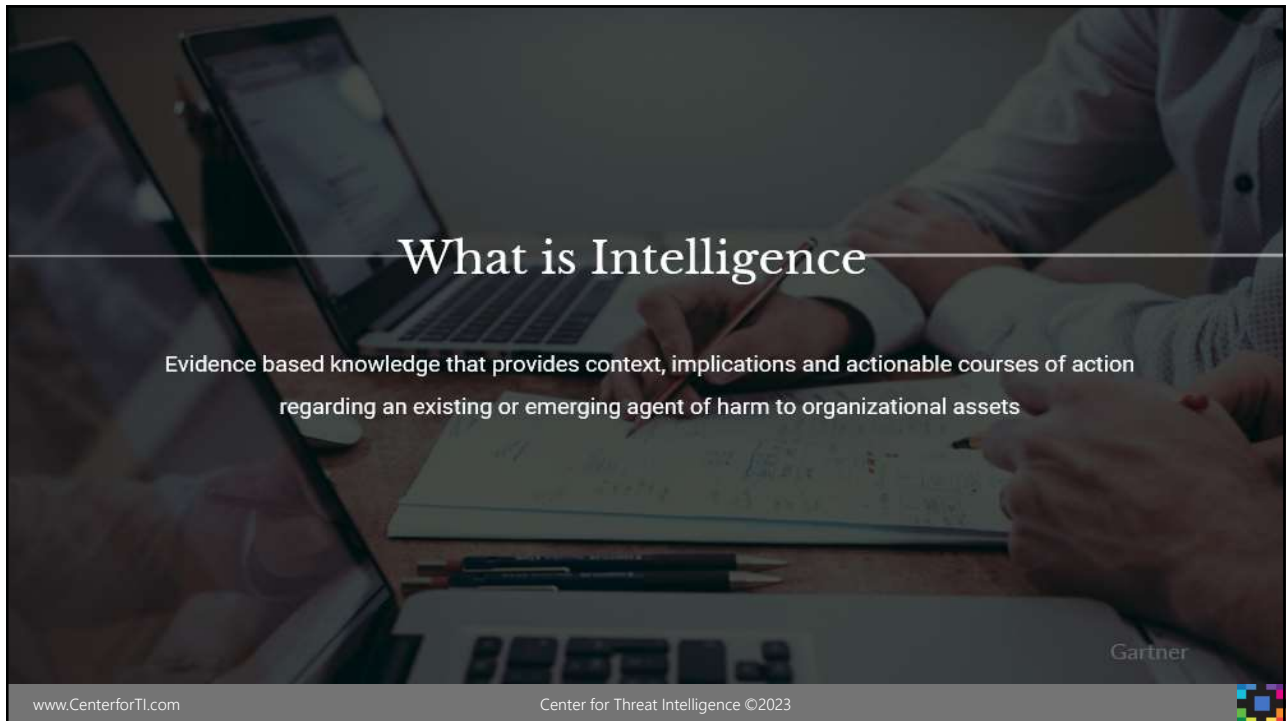


www.CenterforTI.com

Center for Threat Intelligence ©2023



9



What is Intelligence

Evidence based knowledge that provides context, implications and actionable courses of action regarding an existing or emerging agent of harm to organizational assets

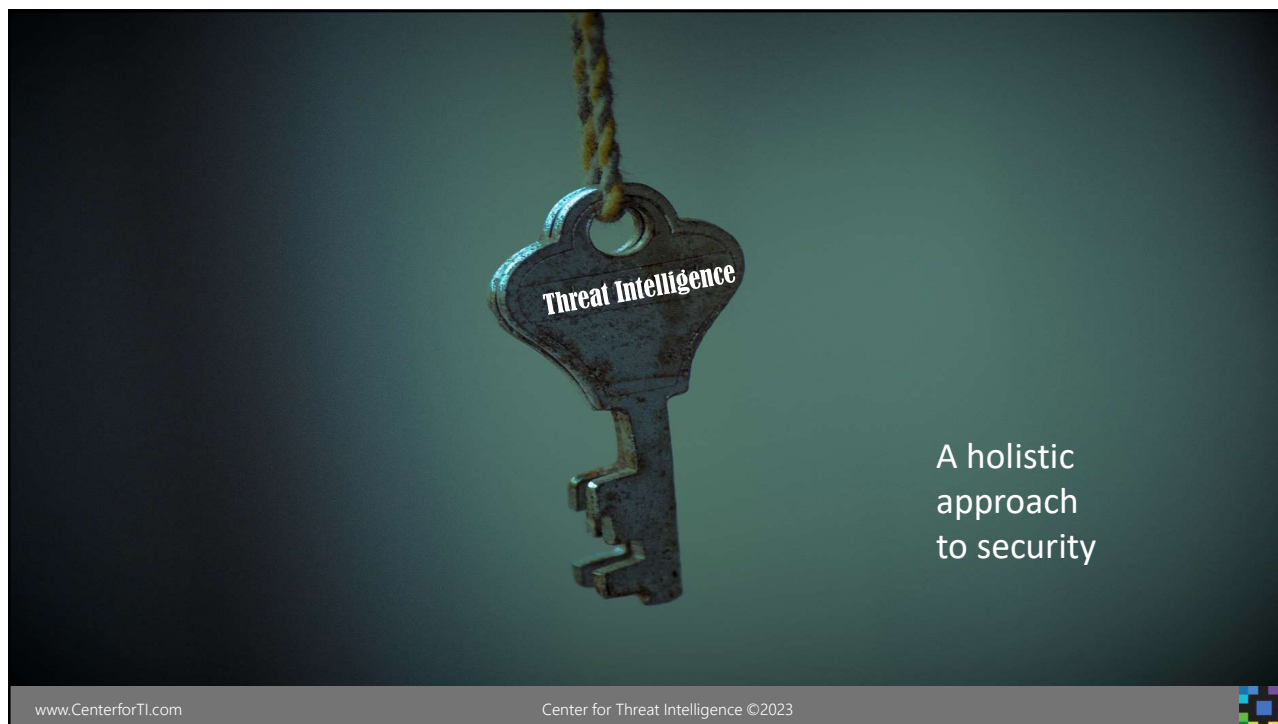
Gartner

www.CenterforTI.com

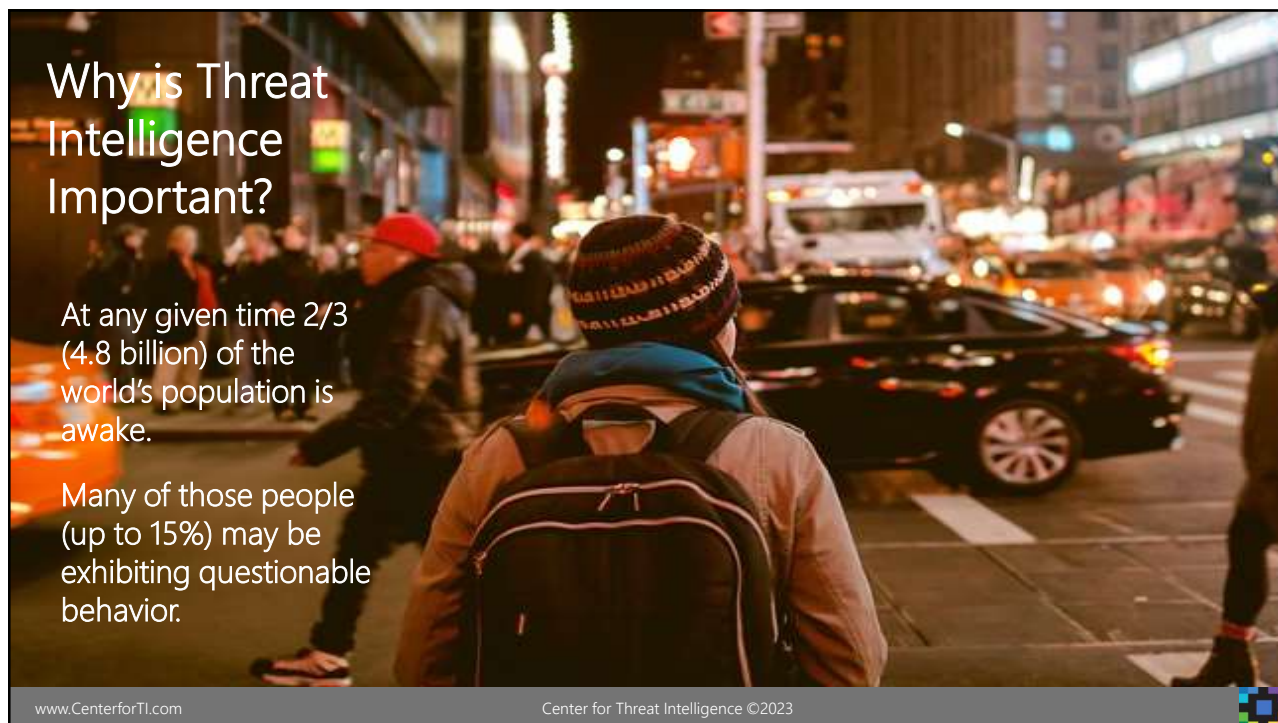
Center for Threat Intelligence ©2023



10



11



12

THE GOAL IS TO ANTICIPATE AND PREVENT

Left of Boom



Right of Boom



13

What Could Possibly Go Wrong?

Right of Boom



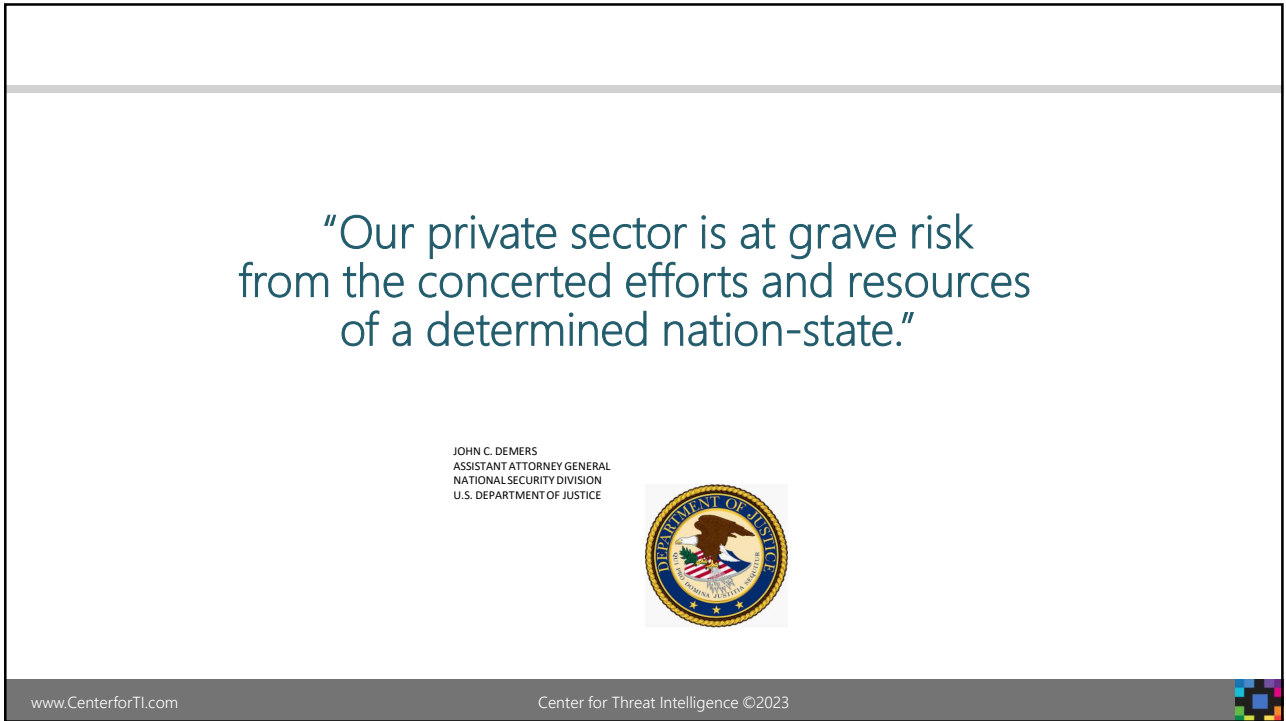
The 6 Very Real Business Impacts of Cyber Attacks FEI Daily



14



15



16

The Goldilocks Effect

- No organization is too BIG
- No organization is too small
- No industry, role or geography is out of bounds
- Any organization or person is “just right”



www.CenterforTI.com

Center for Threat Intelligence ©2023



17

Story Time



www.CenterforTI.com

Center for Threat Intelligence ©2023



18

Know
your
adversaries!



www.CenterforTI.com

Center for Threat Intelligence ©2023



19

When Adversaries Attack...

Focus

Capabilities

Motivation

Tactics

Procedures

Intent



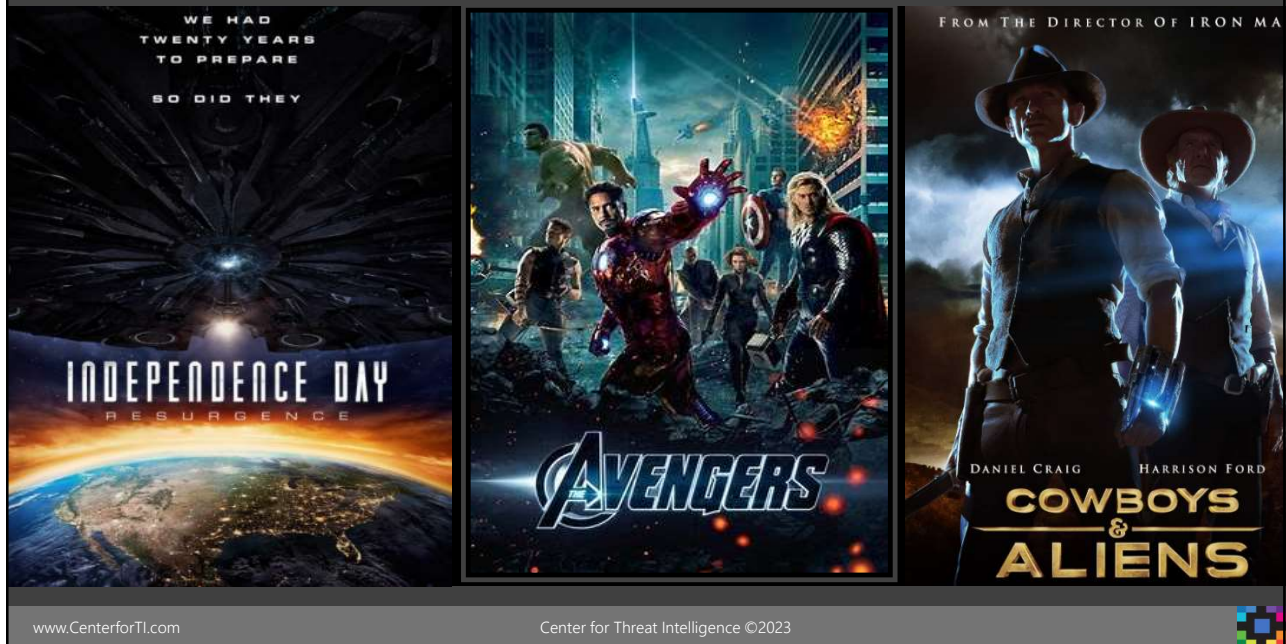
www.CenterforTI.com

Center for Threat Intelligence ©2023



20

Fundamental Aspect of Adversarial Focus




21

Know and Understand Adversarial Tactics



22

FBI Chronicles
Sophisticated Attack



Chinese National Sentenced to Prison for Conspiracy to Steal Trade Secrets

www.CenterforTI.com Center for Threat Intelligence ©2023

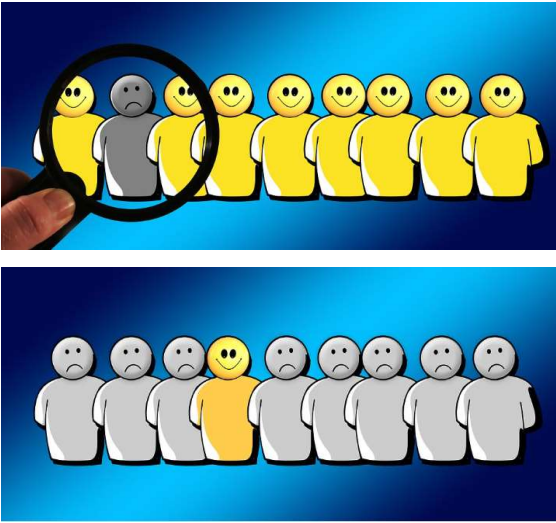
23

Insider Threat

More than 51% of companies are concerned about the unintentional insider attack.

49% of the companies are still worried about malicious insider, which do exist and are a major threat.

67% of the accidental insider threats are exploited through Phishing.



United States Cybersecurity Magazine

www.CenterforTI.com Center for Threat Intelligence ©2023

24

It could happen to your organization.



January 2020

- Employee created false usernames to make direct changes to the Tesla Manufacturing Operating System's (MOS) source code.
- Export large amounts of highly sensitive data to unknown third parties.

MIT
Technology
Review

August 2020

- A Tesla employee thwarted an alleged ransomware plot
- Elon Musk confirmed an employee with alleged promises of a big payout.

WIRED

www.CenterforTI.com

Center for Threat Intelligence ©2023



25

Deception - WWII Ghost Army

Visual deception

Sonic deception

Radio deception

Atmosphere



Wikipedia

www.CenterforTI.com

Center for Threat Intelligence ©2023



26

Sophisticated Attacks

Deception

Chinese company Sinovel had contracted with AMSC for more than \$800 million in products and services to be used for the wind turbines that Sinovel manufactured, sold, and serviced.

Insider Threat

Convinced the head of AMSC Windtec's automation engineering department to leave AMSC Windtec, to join Sinovel, and to steal intellectual property from AMSC.

Devastating Outcomes

According to evidence presented at trial, following the theft, AMSC suffered severe financial hardship. It lost more than \$1 billion in shareholder equity and almost 700 jobs, over half its global workforce.

United States Department of Justice

www.CenterforTI.com

Center for Threat Intelligence ©2023



27



www.CenterforTI.com

Center for Threat Intelligence ©2023



28

Yes it works. Here's how one of our clients did it!



www.CenterforTI.com

Center for Threat Intelligence ©2023



29

Case Study

Challenge: Ongoing Nation State Attacks

- accounts compromised by the threat actor known as the Mabna Group aka Silent Librarian

Focus: Gain Classified information

Motivation: Improve technology/overcome sanctions/expand regional influence

How did they prevent attacks?

- Completed *Enterprise Threat Intelligence Assessment* (ETIA)
Identifies key adversaries, focus, motivation, capabilities, etc.
- Threat Intelligence Training
- Identified Silent Librarian's Techniques, Tactics and Procedures (TTPs)
- Developed Signposts and Early Warning indicators using Sensemaking techniques (Center for Threat Intelligence Training)
- Created a Monitoring System of known TTPs to warn of an upcoming attack and became proficient at blocking incoming attacks before they were launched.

Success!

The monitoring system is still running today. So far, 6+ attacks have been stopped!

"I credit Janet and her team for giving us the wherewithal to pull this off."

Director of
Cyber Intelligence

www.CenterforTI.com

Center for Threat Intelligence ©2023



30

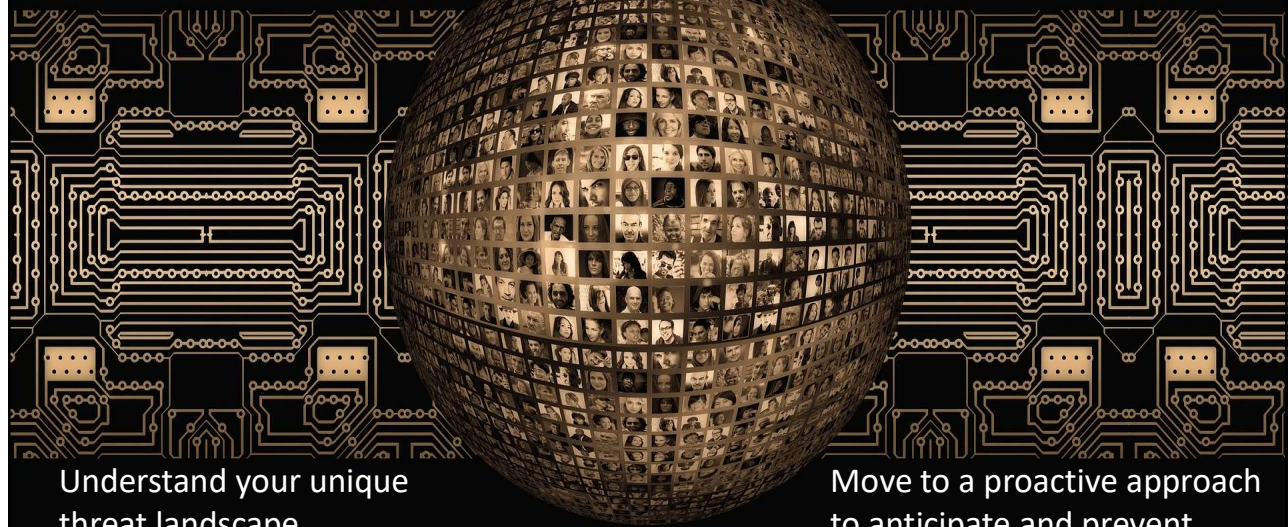


31



32

Create an Enterprise-Wide Threat Intelligence Environment



Understand your unique threat landscape

Move to a proactive approach to anticipate and prevent

www.CenterforTI.com

Center for Threat Intelligence ©2023



33

Where do you start?



www.CenterforTI.com

Center for Threat Intelligence ©2023



34

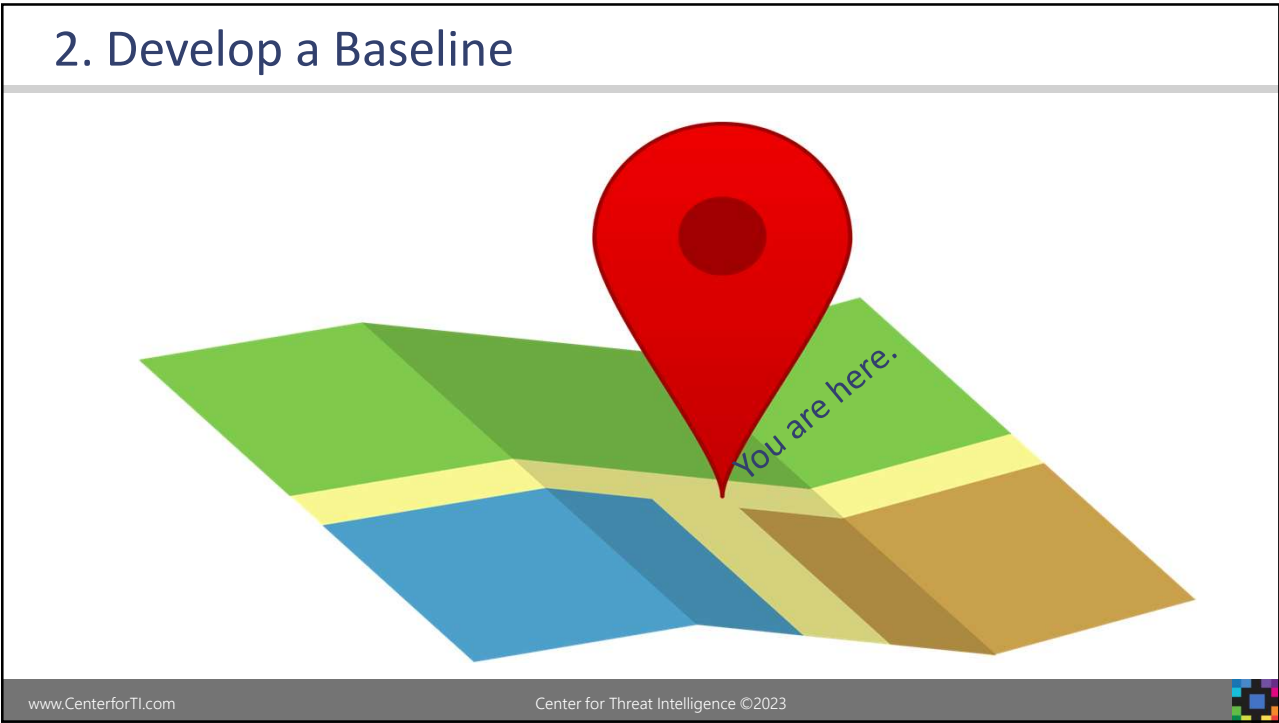


1. Executive Approval and Commitment

www.CenterforTI.com

Center for Threat Intelligence ©2023

35



2. Develop a Baseline

www.CenterforTI.com

Center for Threat Intelligence ©2023

36

Enterprise threat intelligence assessment

- **Threat profiling:** Defines sophistication of actors targeting your organization
- **Adversarial focus:** Identifies assets of interest within your organization and strategies and tactics used for attacks
- **Gap analysis for threat mitigation:** Identifies current controls in place and potential gaps
- **Threat Maturity Scorecard:** Establishes a baseline of current threat intelligence capabilities
- **Threat Map:** Maps threats to targets and controls

Capability Model

Capability	Low Maturity	Intermediate Maturity	Mature	Highly Mature
Information	Ad hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	No dedicated program	Basic, tactical and ad-hoc	Operationalized program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program
Threat Intelligence	Ad-hoc program	Operationalized program	Comprehensive program	Advanced program

©2022 Center for Threat Intelligence

www.CenterforTI.com

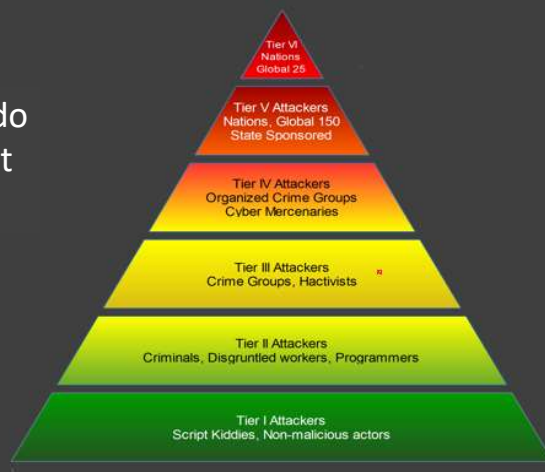
Center for Threat Intelligence ©2023



37

Enterprise Threat Intelligence Assessment: Adversarial Profiles

What assets do you have, that "they" want?



Significant

Nuisance

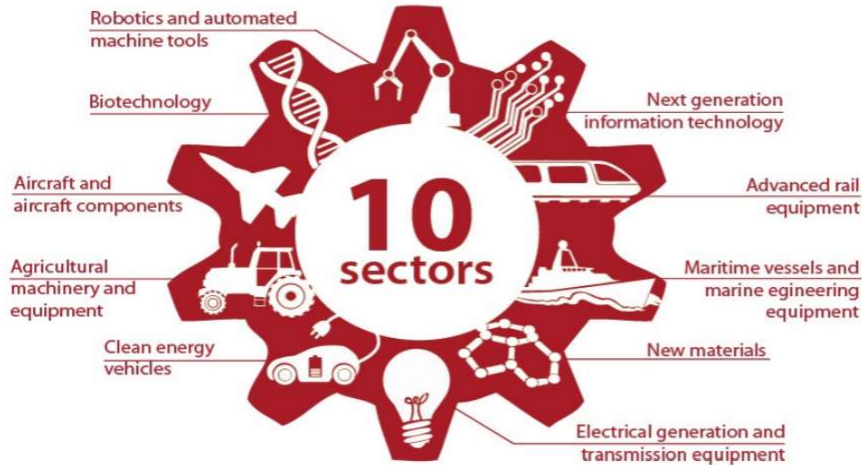
www.CenterforTI.com

Center for Threat Intelligence ©2023



38

Determine if you are a target?



Made in China 2025
US Department of Justice

www.CenterforTI.com

Center for Threat Intelligence ©2023

39

3. Build an intelligence strategy

Analyze threat actor and specific to your organization.

Understand adversarial intent and capability.

Develop agile strategy to meet new evolving threat.

Identify attribution by understanding threat focus, intent and capability, in order to effectively respond and initiate proactive measures in securing assets.

Determine shifting threat landscapes that may drastically impact organization.

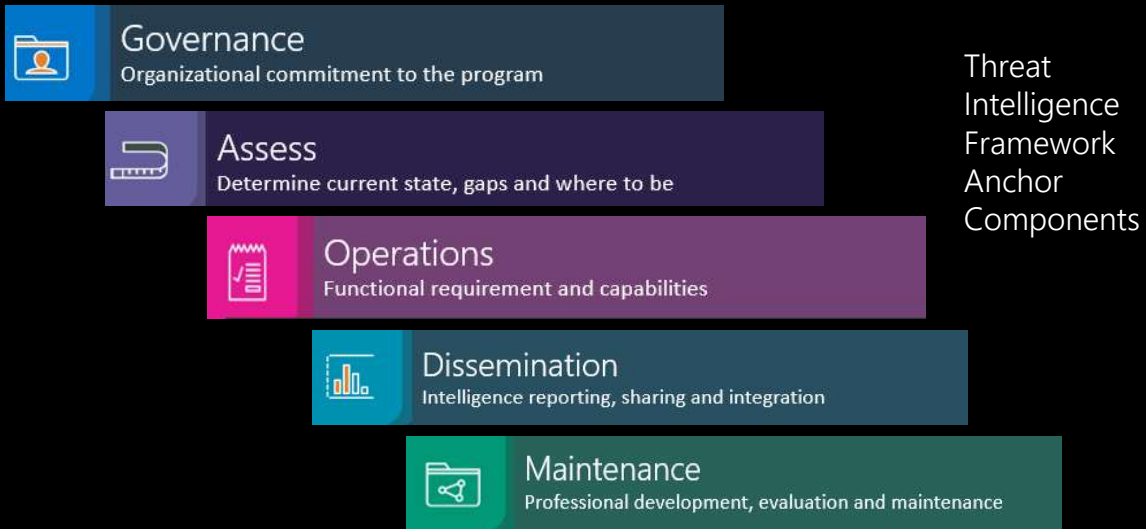
Discover disparate events and shifts at a high level, such as changes in technology, geo-political and economic events, threat actor strategy, shifting in targeting and capabilities.

www.CenterforTI.com

Center for Threat Intelligence ©2023

40

4. Incorporate a framework



41

5. Create an Enhanced Communication Plan



42

6. Train everyone – all departments



www.CenterforTI.com

Center for Threat Intelligence ©2023



43

Time is ticking...




1. Executive Approval and Commitment
2. Develop a Baseline:
Enterprise Threat Intelligence
Assessment
3. Build an Intelligence
Strategy
4. Incorporate a Framework
5. Create a Communication Plan
include the entire organization
6. Get people trained

www.CenterforTI.com

Center for Threat Intelligence ©2023



44



CHALLENGES

- Limited threat intelligence experts and resources
- Nation States have a wealth of resources
- Threat intelligence experts are very expensive
- Nation State and organized crime have the money to fund attacks
- Limited corporate-wide threat intelligence processes in place
- Your people may need training to get ahead of your adversaries and change the processes
- Experts still need to analyze and provide relevance from threat intelligence tools
- Hard to justify business ROI when you are preventing attacks

www.CenterforTI.com Center for Threat Intelligence ©2023

45

Benefits of an in-house threat intelligence

- **Protects current investments**
 - Adds value to current security and risk management programs
- **Cost management**
 - Significant savings when intelligence mitigates risk and prevents attacks from happening
- **Brand integrity and recognition**
- **Reduces loss**
 - Records, funds, critical services, intellectual property
- **Demonstrates executive level due care**
- **Helps enhance your career by making you more valuable for promotions and keeping your job!**

www.CenterforTI.com Center for Threat Intelligence ©2023

46



www.CenterforTI.com

Center for Threat Intelligence ©2023



47



**“ONE PERSON CAN MAKE A DIFFERENCE
AND EVERYONE SHOULD TRY”** JFK

www.CenterforTI.com

Center for Threat Intelligence ©2023



48

You are that person!

- Think out of the box
- Introduce an Enterprise Intelligence Approach
- Build Holistic Security in your organization and....
- STAY....

LEFT OF BOOM

www.CenterforTI.com Center for Threat Intelligence ©2023

49

Questions?

www.CenterforTI.com Center for Threat Intelligence ©2023


50

Thank you!

Janet Lawless, CTIS
CEO/Founder
Center for Threat Intelligence
Chair ASIS Puget Sound Chapter

jlawless@CenterforTI.com
www.centerforti.com

www.CenterforTI.com



Center for
Threat Intelligence

©2023 Center for Threat Intelligence