UNECE

United Nations Economic Commission for Europe
Committee on Sustainable Energy | Group of Experts on Cleaner Electricity Systems
Nineteenth Annual Session | 3. – 4. October 2023

Reliability and cyber resiliency of smart integrated energy systems

FORTINET

Stefan Züger, Director Systems Engineering at Fortinet Switzerland
szueger@fortinet.com

Agenda

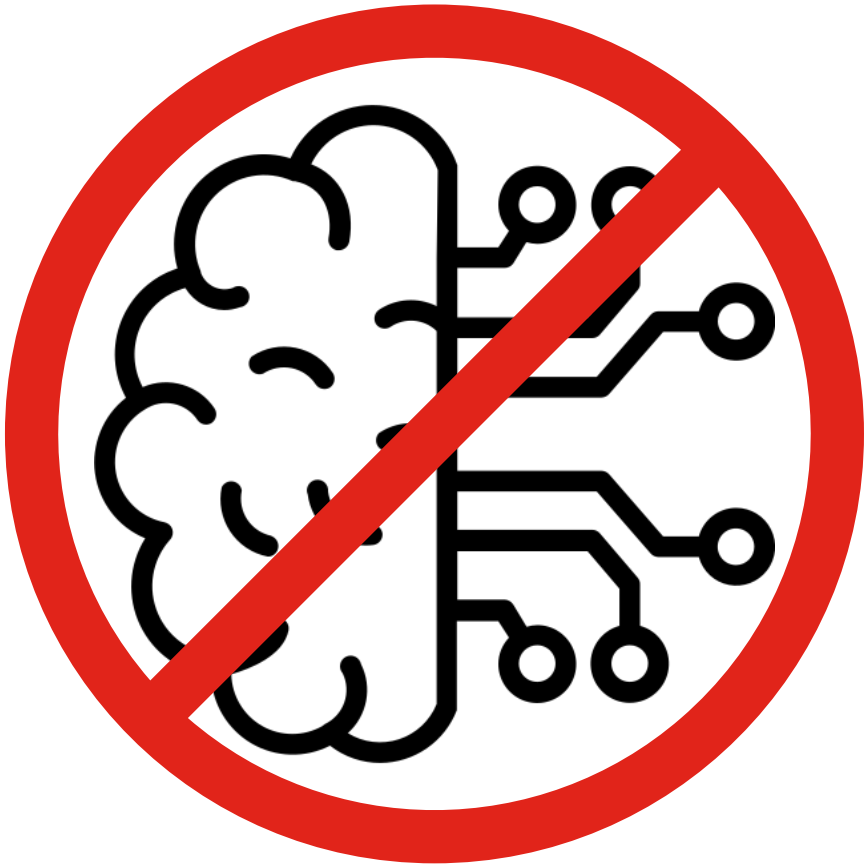
About Fortinet

Cyber Challenges in the Power & Utilities Industry

Cyber Defense Standards

Cyber Defense Best Practices

Warning! This is not an AI pitch!

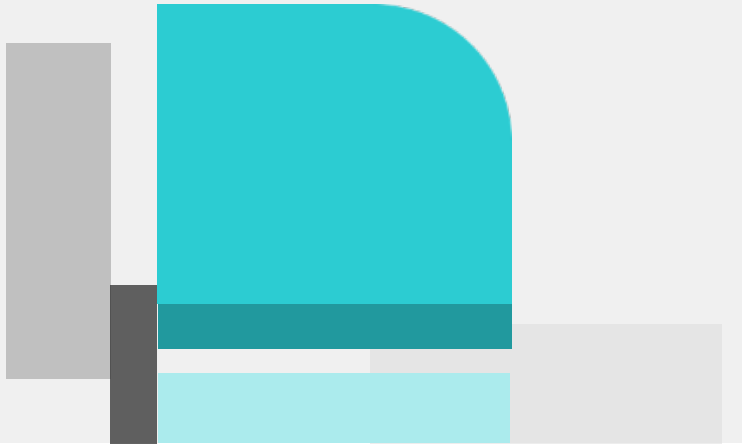


Artificial Intelligence and Machine Learning are powerful tools that render both the attacker's and the defender's tool box more powerful and scalable.

However, I will not focus on the application of AI itself – consider it as an integral part for every concept and technology discussed.

About Fortinet

Cybersecurity, everywhere you need it.



Fortinet Company Profile / Global Presence

Fortinet: Trusted by 660k customers worldwide

$59.38B
Market Capitalization

$5.59B+
2022 Billings

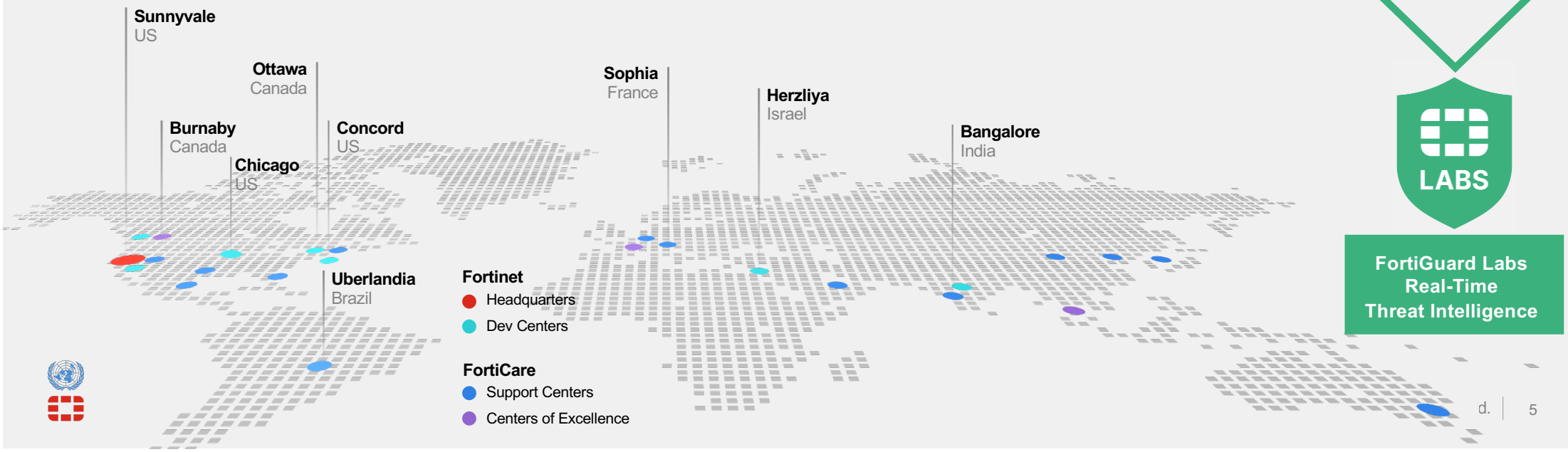
11,500+
Employees

1,285
Patents Globally

660,000+
Customers Worldwide

8.8M+
Global Firewall Shipments

5.6M
Active Devices



FortiGuard Labs: Threat Intelligence & Security Services

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. We develop and utilize leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence.

Global Leadership & Collaboration:

CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NCI AGENCY

FortiGuard Labs Real-Time Threat Intelligence

FortiGuard AI-Powered Security Services

FortiGuard Expert Services

500+ FortiGuard Labs Global Threat Hunters and Researchers

600K+ Hours of Threat Research a Year

100+B global security events analyzed per day

Sharing intelligence with the industry

Original CTA Co-Founder (2014) / charter member / 37 industry players

- Sharing indicators of compromise daily - more than 10 M observables per month
- Sharing insights before disclosed to the public
- In average Fortinet is comtributing 10% of the data shared and was #1 in power rankings in 2022

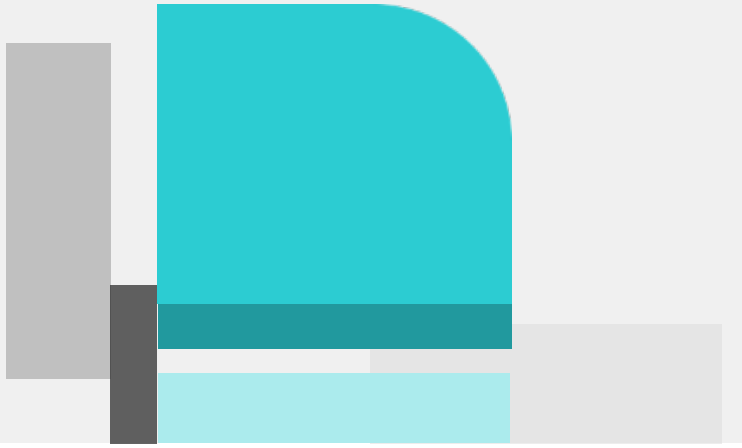
CYBER THREAT ALLIANCE

Global Leadership & Collaboration:

CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NCI AGENCY

500+	FortiGuard Labs Global Threat Hunters and Researchers	**600K+**	Hours of Threat Research a Year	**100+B**	global security events analyzed per day

Cyber Challenges in the Power & Utilities Industry



Same, same: Cyber Crime is a standardized business

PHISHING

MALWARE

RANSOMWARE

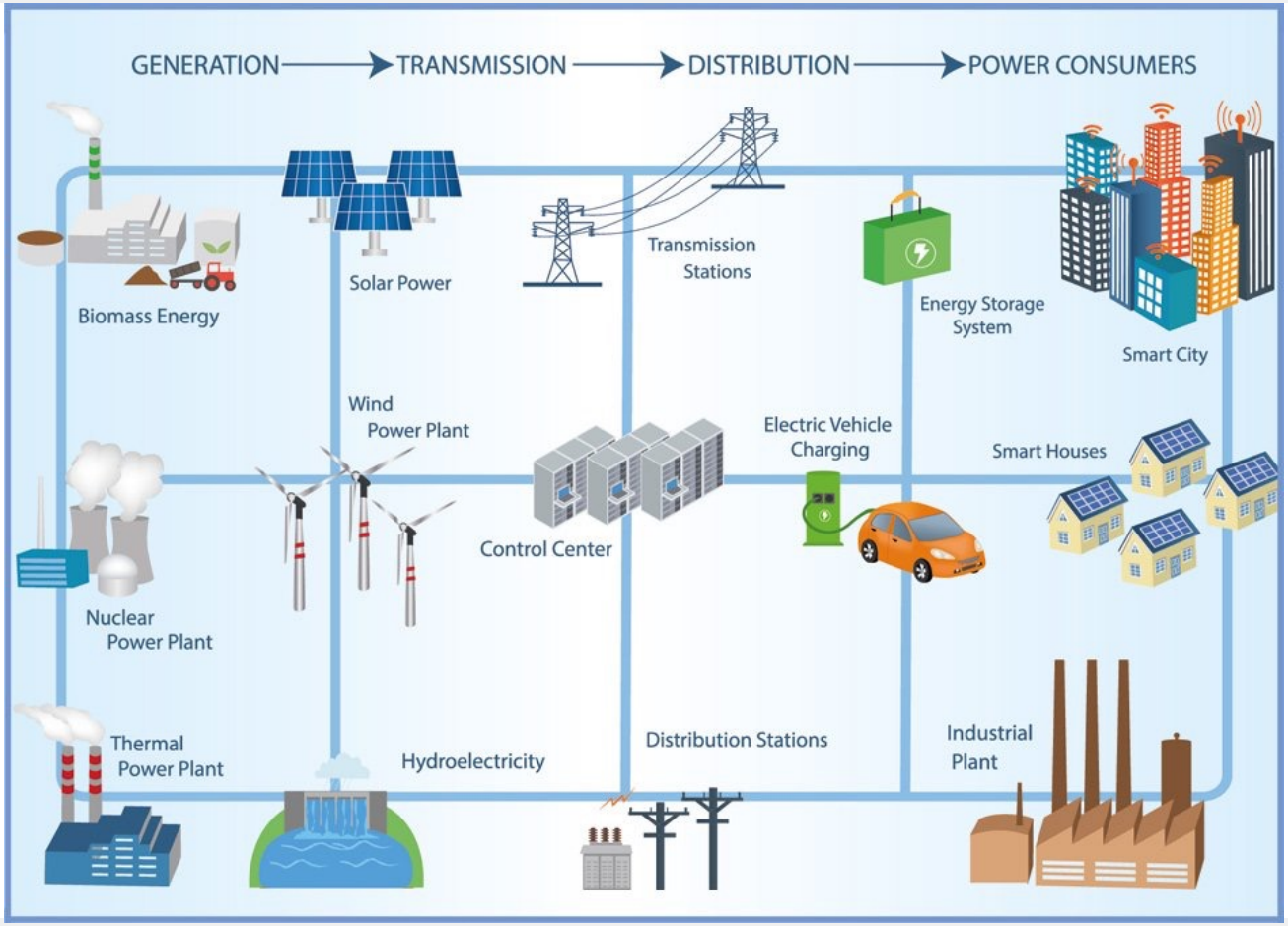
INTERNAL THREATS

DDOS

DEVICE VULNERABILITIES

- Cyber Crime has become a highly profitable business, with its own best practices, business models, cartels and service providers.
- We have seen threats customized for industrial (OT) environments (Stuxnet, NotPetyia, Triton), Oldsmar.
- However, the majority of threats we observe are not distinguishing between target industries.

… but different: a constantly increasing attack surface



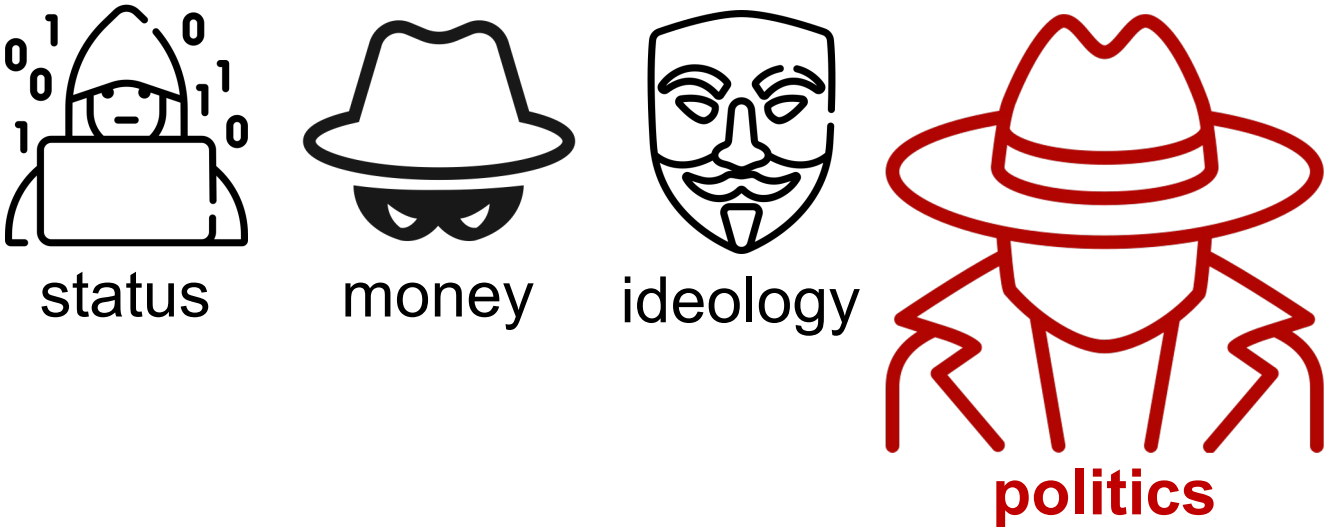
digitalization of power generation, distribution, transport

- in the old days, everything was one way
- now everything happens from all sides and all the time

supply chain risks

- more and smaller utilities
- private players contributing to power production (supply chain risks)
- smart grid

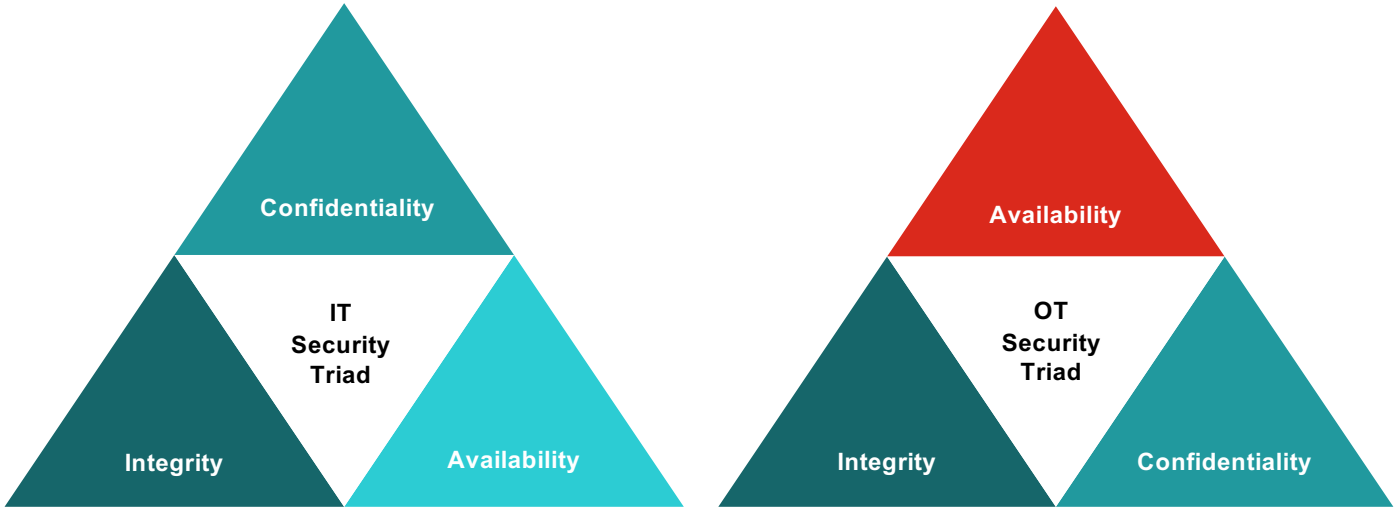
… but different: highly motivated threat actors



threat actors driven by ideology (hacktivists) or politics (nation state activists) tend to

- be much more persistent
- take more time exploring the weaknesses before exploiting them
- remain in your system for a long time - undetected

… but different: engineering mindset



Source: dqchannels.com,

an IT engineer will follow the CIA triad:

- confidentiality
- integrity
- availability

OT engineers follow the reversed credo:

- **AVAILABILITY**
- integrity
- confidentiality

… but different: legacy systems


Source: iStock Pictures, Michael Jung

modern systems should be built with inherent security

- not always the case – dependencies in code libraries from other libraries – Log4J

legacy systems are not

- they often provide no inherent way to cyber-protect them
- if security cannot built in, it must be built around

Cyber Defense Standards

NIST framework: Build your Defense Strategy

National Institute of Standards and Technology
U.S. Department of Commerce

Source: https://www.nist.gov/cyberframework
Drawing © Axians IT Services AG

The NIST Cybersecurity Framework is a set of guidelines and best practices to help organizations manage and improve their cybersecurity risk.

It consists of five core functions, providing a structured approach to enhancing cybersecurity resilience.

MITRE ATT&CK: Know How Attackers Work

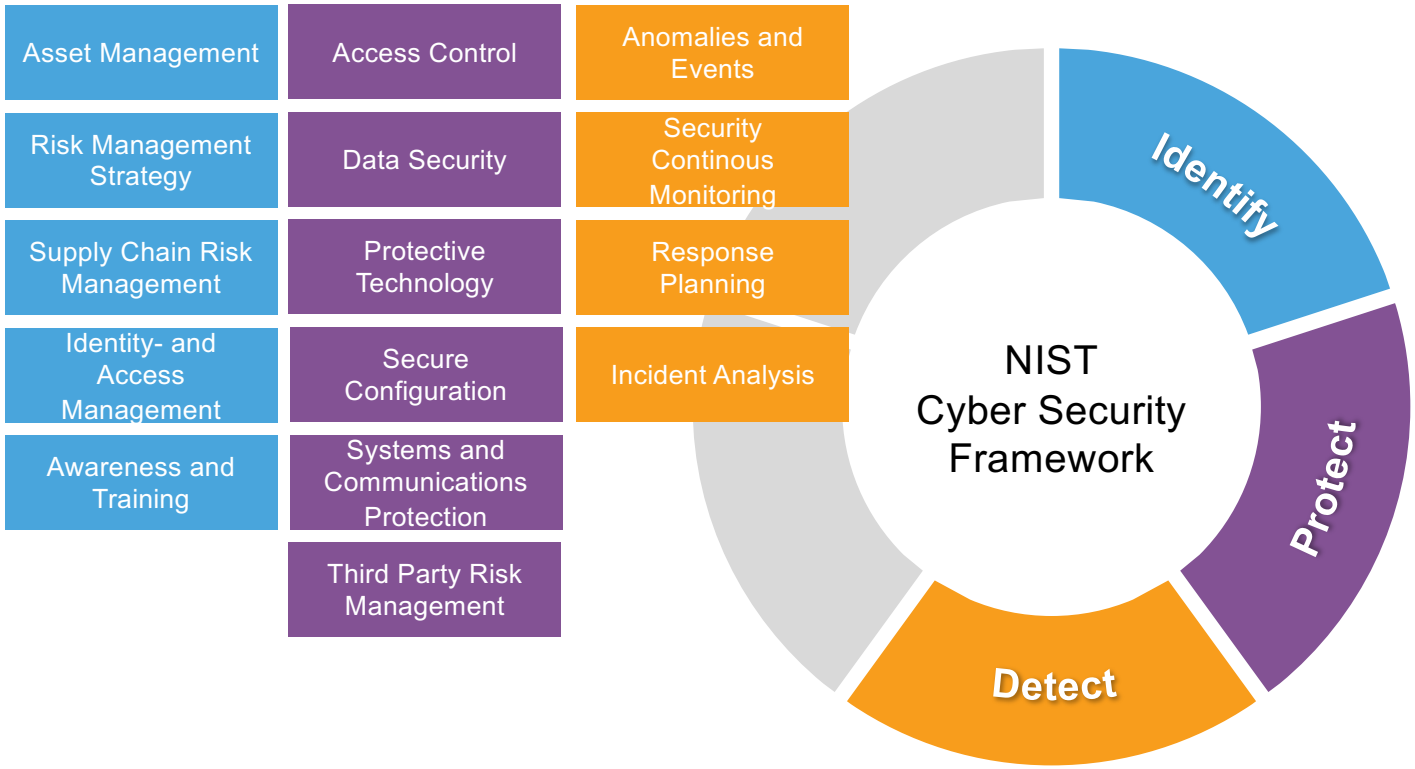
ATT&CK®

Source: https://attack.mitre.org/

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

80% of defensive measures are in Identify, Protect and Detect



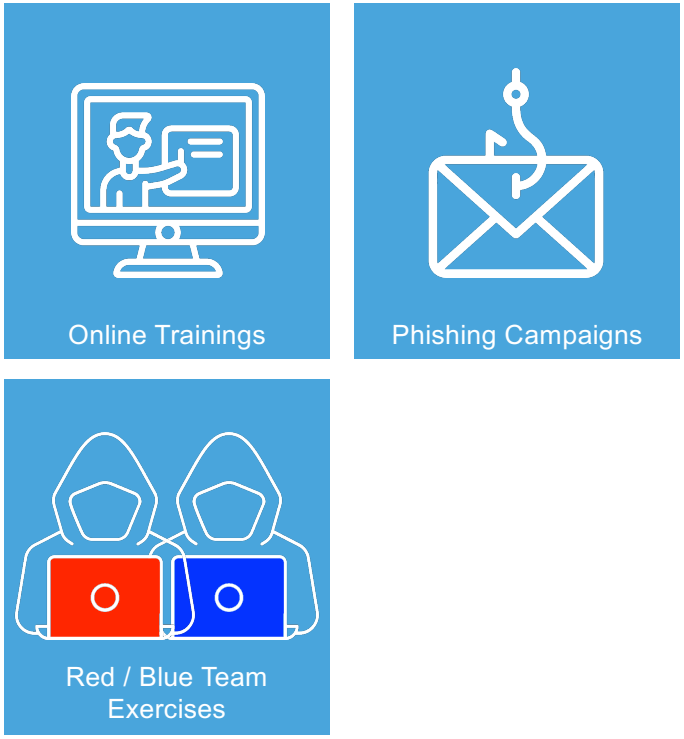
- 80% of the measures to be taken are in the first three sections
- **Identify**: understanding and managing cybersecurity risk
- **Protect**: implementing safeguards and protective measures
- **Detect**: identifying and promptly detecting cybersecurity incidents or anomalies

Cyber Defense Best Practices

Identify: Information Gathering

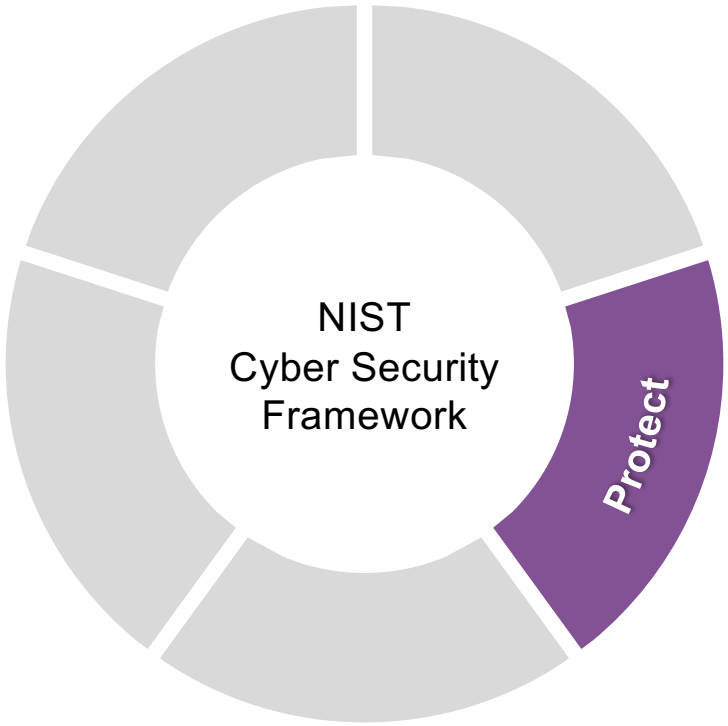
collect information on the actual threat landscape relevant for your industry

Identify: Awareness Training



empower your staff partners and contractors with knowledge and skills to recognize, prevent, and respond to cybersecurity threats, enhancing overall organizational security.

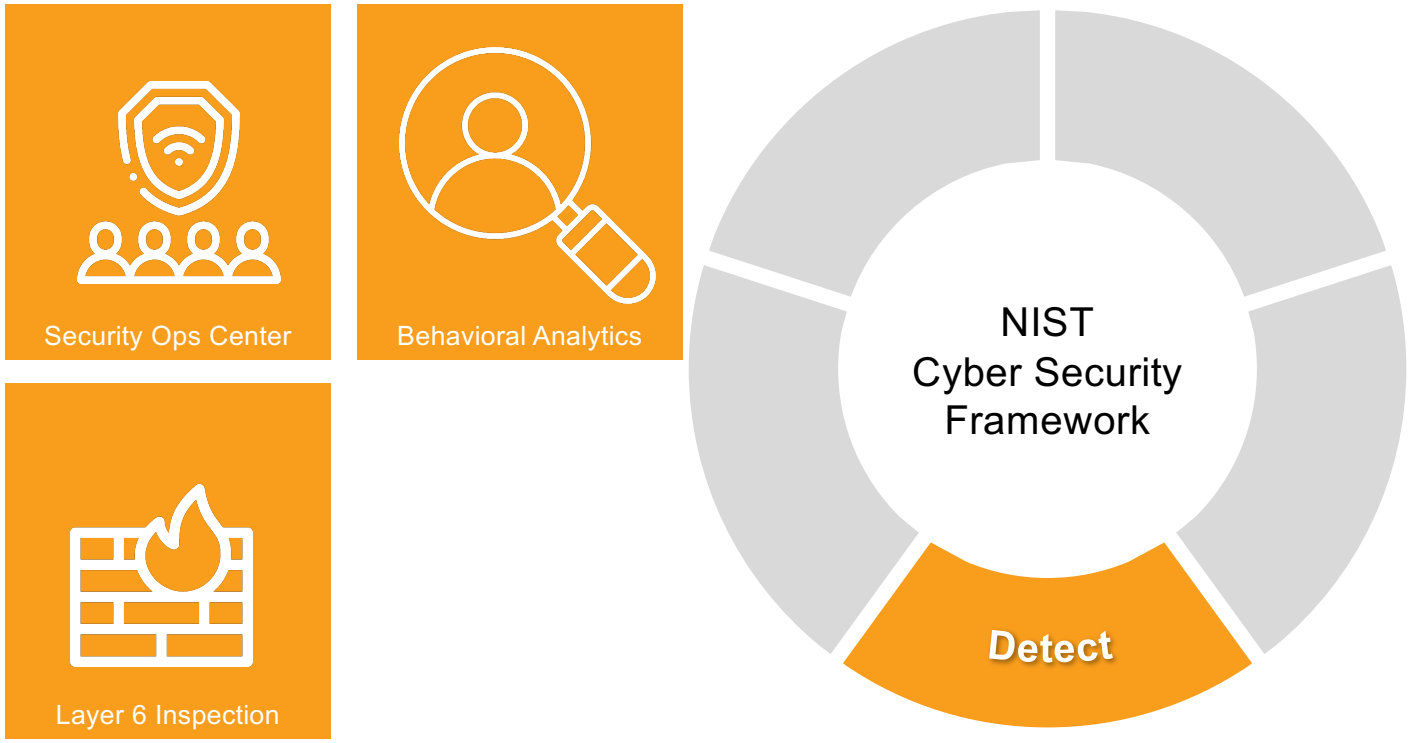
Protect: Reduce the Attack Surface



minimize vulnerabilities or potential points of entry for cyberattacks

enhance security by limiting exposed or exploitable areas in your system or network.

Detect: Identify Incidents and Anomalies



recognize unusual or potentially harmful events within a system or dataset,

enable prompt response and investigation for security or operational purposes

Conclusion

the danger is real

dependencies and digitalization have extended the attack surface

Cyber Defense Standards are in place

Cyber Defense technologies exist and keep developing


FORTINET