OPSWAT.

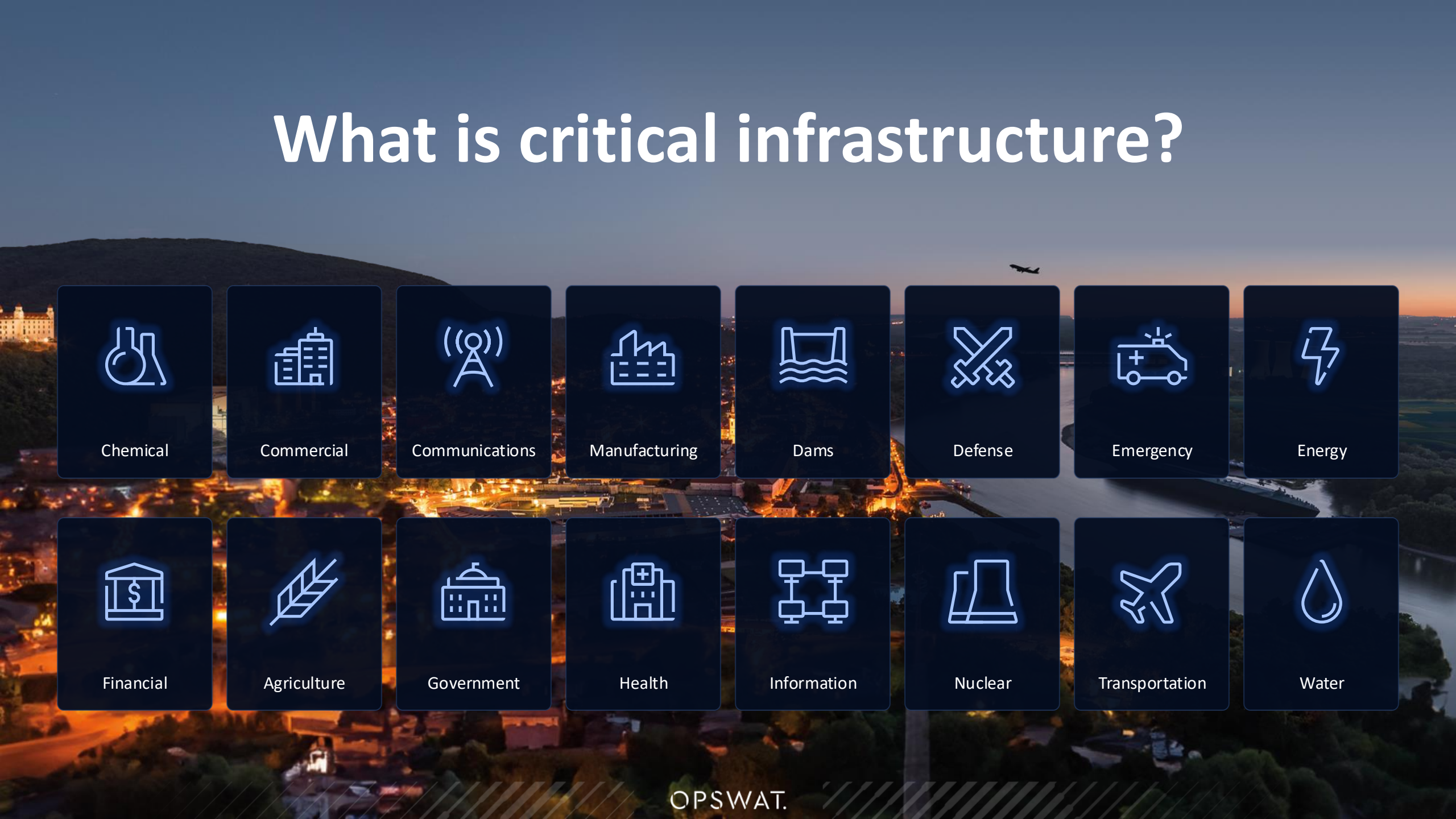
Cybersecurity Solutions for Critical Infrastructure

INFORMATION SECURITY FOR NATIONAL DATA INFRASTRUCTURE AND DIGITAL PLATFORM

Prepared for: VIETNAM INFORMATION SECURITY DAY 2024
Prepared by: Cuong La - GM & VP of R&D, OPSWAT Vietnam
Date: November 21, 2024


OPSWAT.
We Protect the World's Critical Infrastructure

What is critical infrastructure?



Notable attacks on Critical OT/ ICS

For Critical OT, Nation-state threats are ever-present; held back only by the socio-political climate

Cost of an OT Cyber Incident

OT Cyber Incidents can result in up to 15 days of downtime, loss of production, reputation damage, and recovery costs

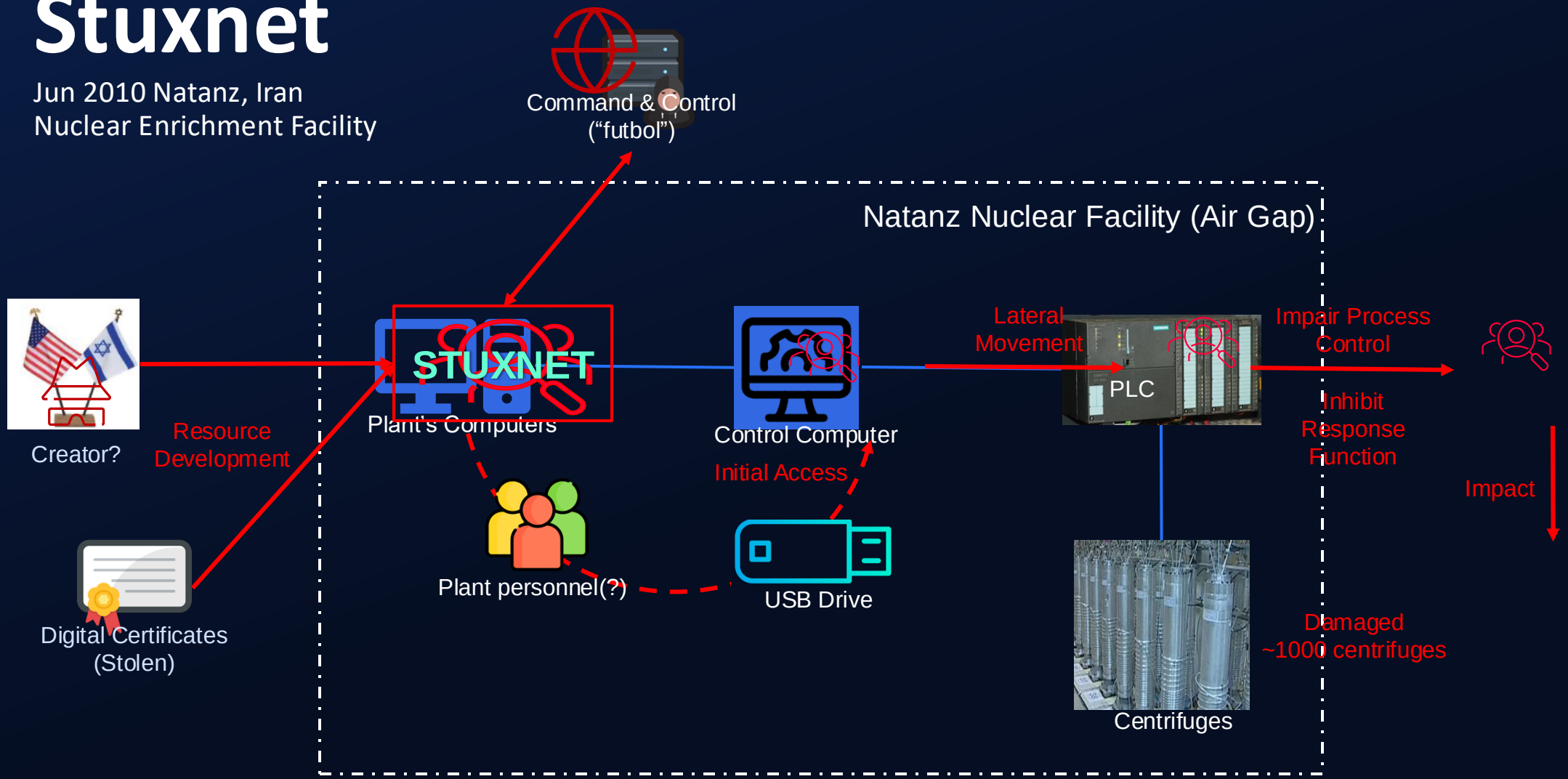
1 Cyber Incident = 1.3 hurricanes

1 Cyber Incident = 20 Major Storms

ANATOMY OF A CPS ATTACK

Stuxnet

Jun 2010 Natanz, Iran
Nuclear Enrichment Facility



ANATOMY OF A CPS ATTACK

FrostyGoop

April 2023 – January 2024 Lviv, Ukraine – Heating Utility Systems

Investigation ongoing

"Air Gap"

Vulnerable Router

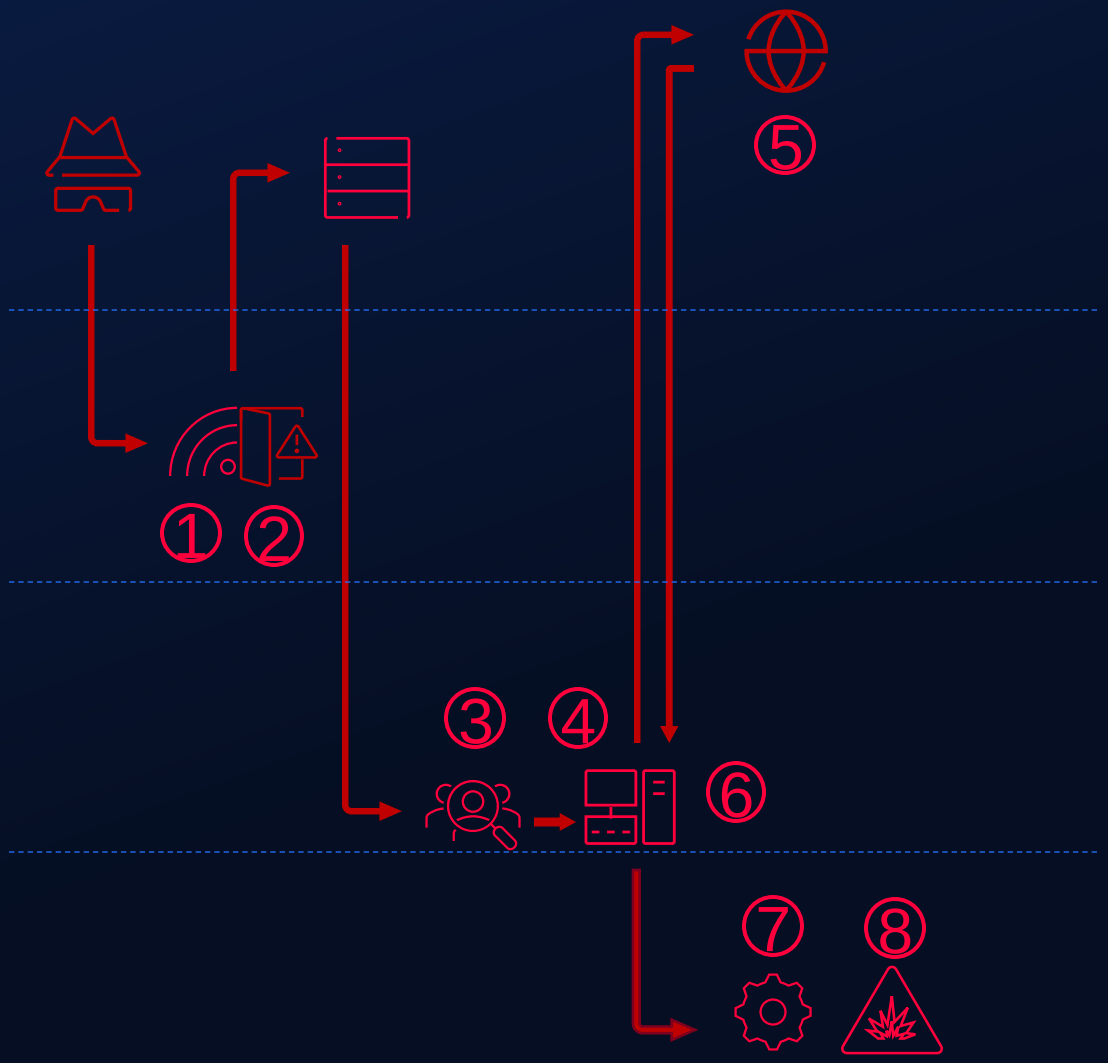
Operations / Management Server

Industrial Control Process

"What could go wrong?"

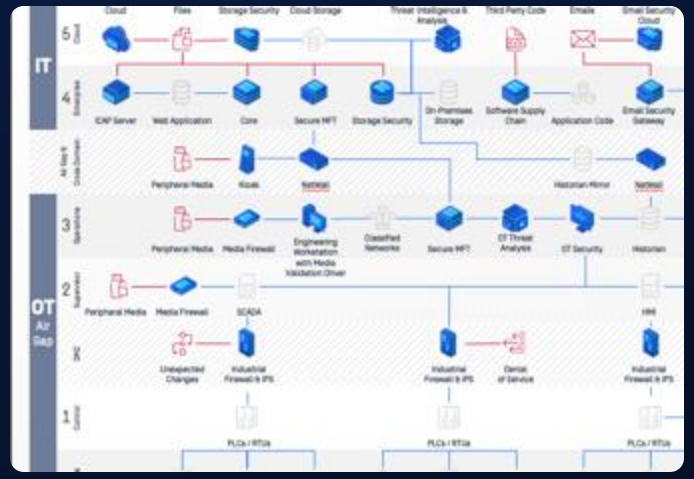
ANATOMY OF A CPS ATTACK

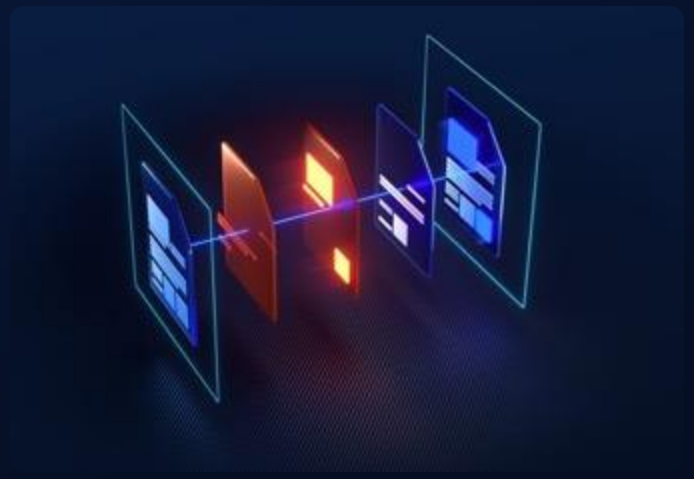
FrostyGoop



1. Threat actors exploit a vulnerability in external facing MikroTik router
2. Deploy a webshell with tunneling accessed by a TOR Address
3. Retrieve Security Account Manager (SAM) registry hive
4. Deploy and test FrostyGoop Malware (Golang binary using JSON configs)
5. Threat Actors establish connection to Moscow Based IP Addresses
6. Threat Actors send malicious Modbus commands to FrostyGoop
7. Commands are sent directly to the heating system controllers, reporting false measurements
8. Process disables heat based on faulty measurements

Protecting the World's Critical Infrastructure





Comprehensive Platform

- Covers IT, OT & ICS Use Cases
- Supports Air-gapped Networks
- Cloud, Software and Hardware
- 21 Products and Growing

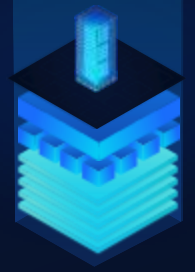
Purpose-Built Technologies

- Prevention Not Based on Detection (CDR)
- Multi-Antivirus Engine Scanning
- File Based Vulnerabilities
- Country of Origin Detection
- Malware Analysis for IT/OT
- CIP Protocol Support

Training Academy

- Practical Online Training and Certification
- Regional CIP Labs

MetaDefender Platform



Files

Emails

Endpoints

Peripheral Media

Cloud/Web

MetaScan®

Deep CDR

Adaptive Sandbox

Proactive DLP

File-based Vulnerability Assessment

Threat Intelligence

SBOM

Country of Origin

Air-Gap On-Premises Cloud

Core

ICAP Server

Storage Security

Email Security

Software Supply Chain

Kiosk

Drive

Media Firewall

Managed File Transfer

IT-OT Access

Endpoint

Uni / Bidirectional Gateways + Data Diode

OT Security

Industrial Firewall

User Endpoints

Applications

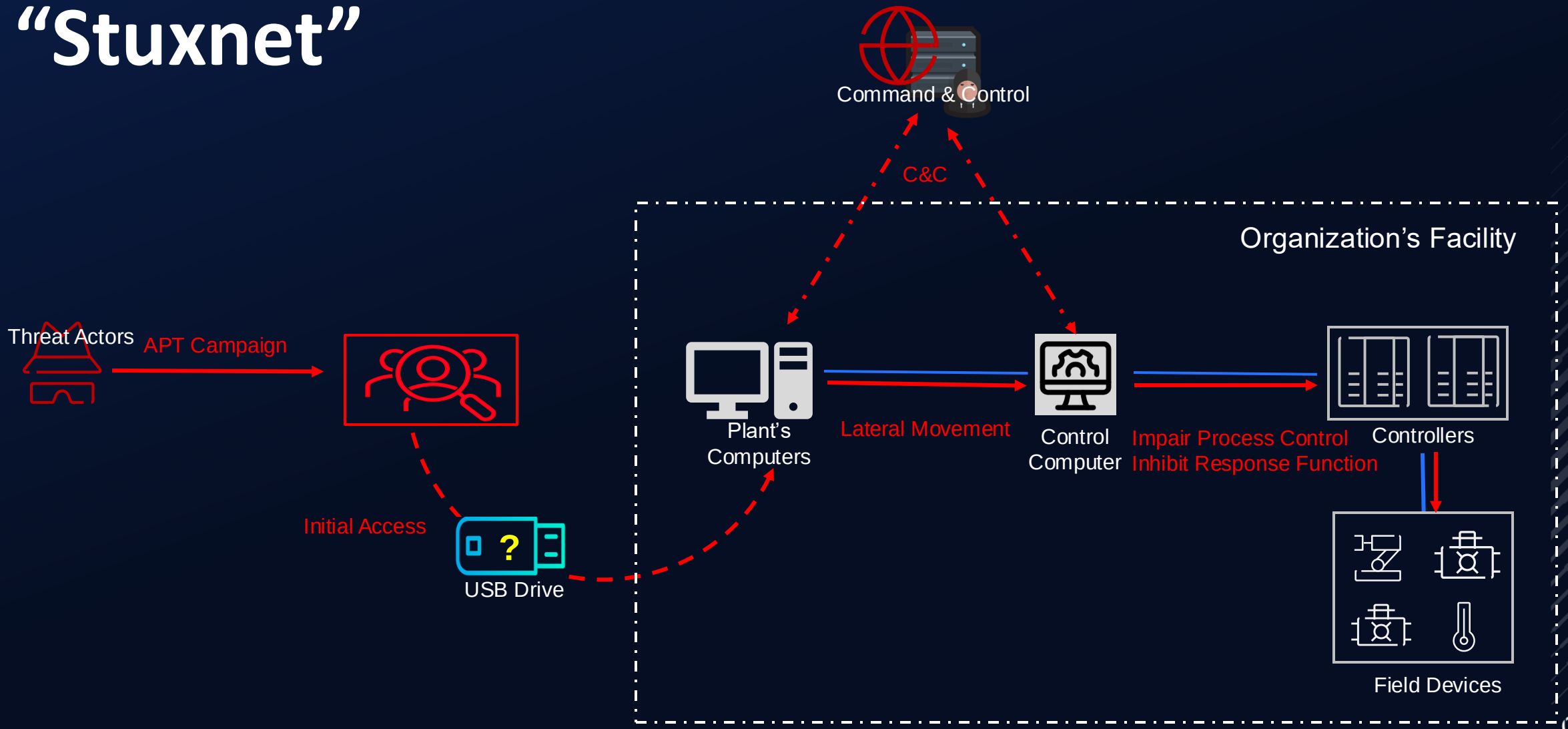
Storage

Other Organizations

OPSWAT.

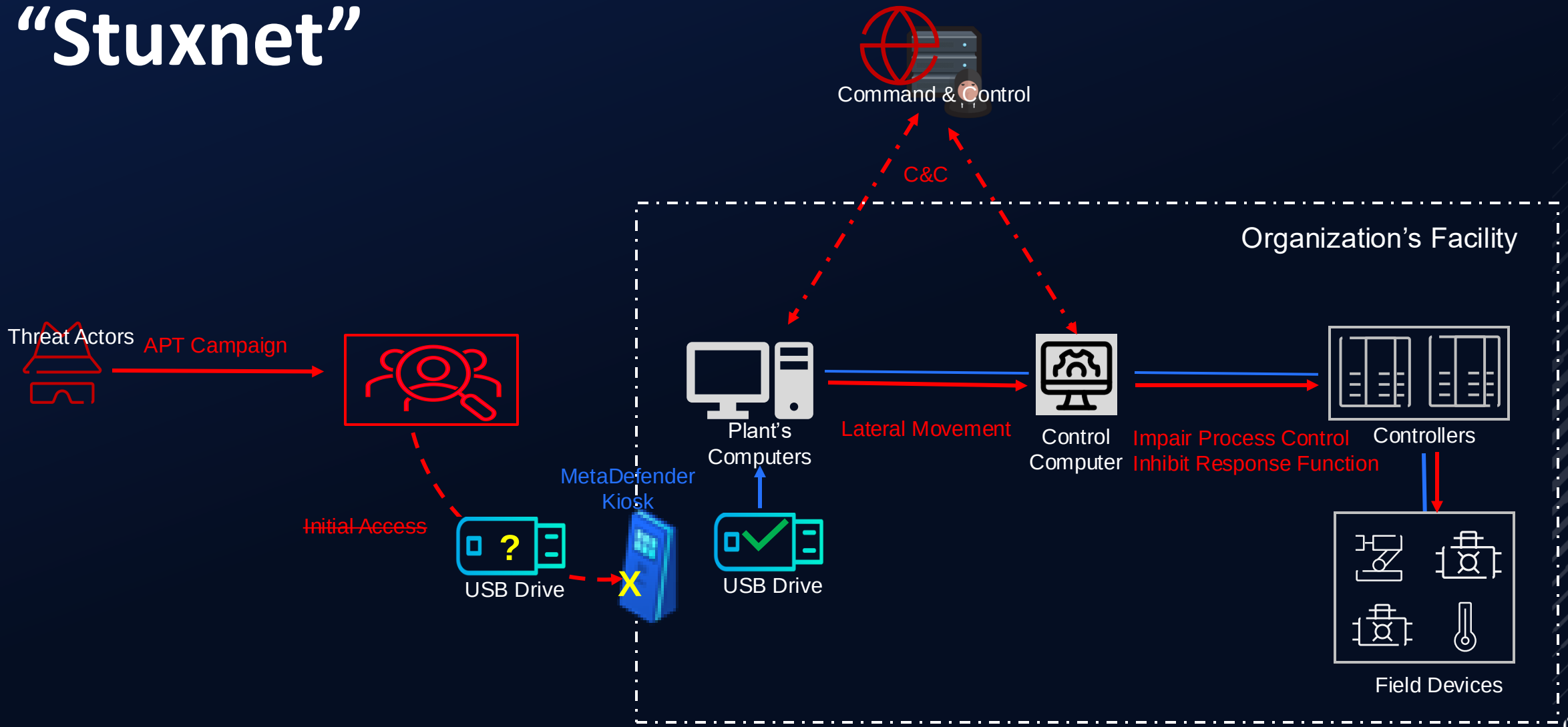
OPSWAT SOLUTIONS

Prevent “Stuxnet”



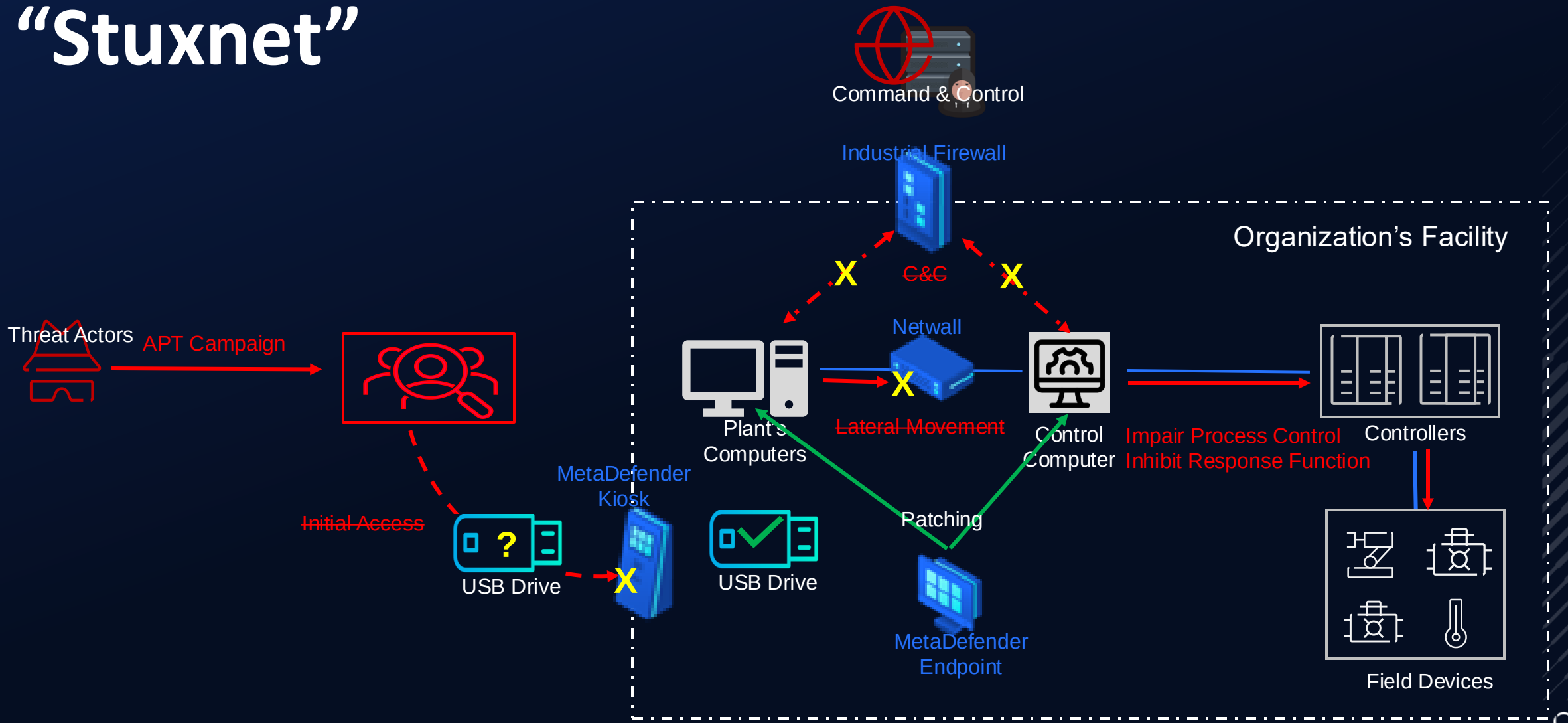
OPSWAT SOLUTIONS

Prevent “Stuxnet”



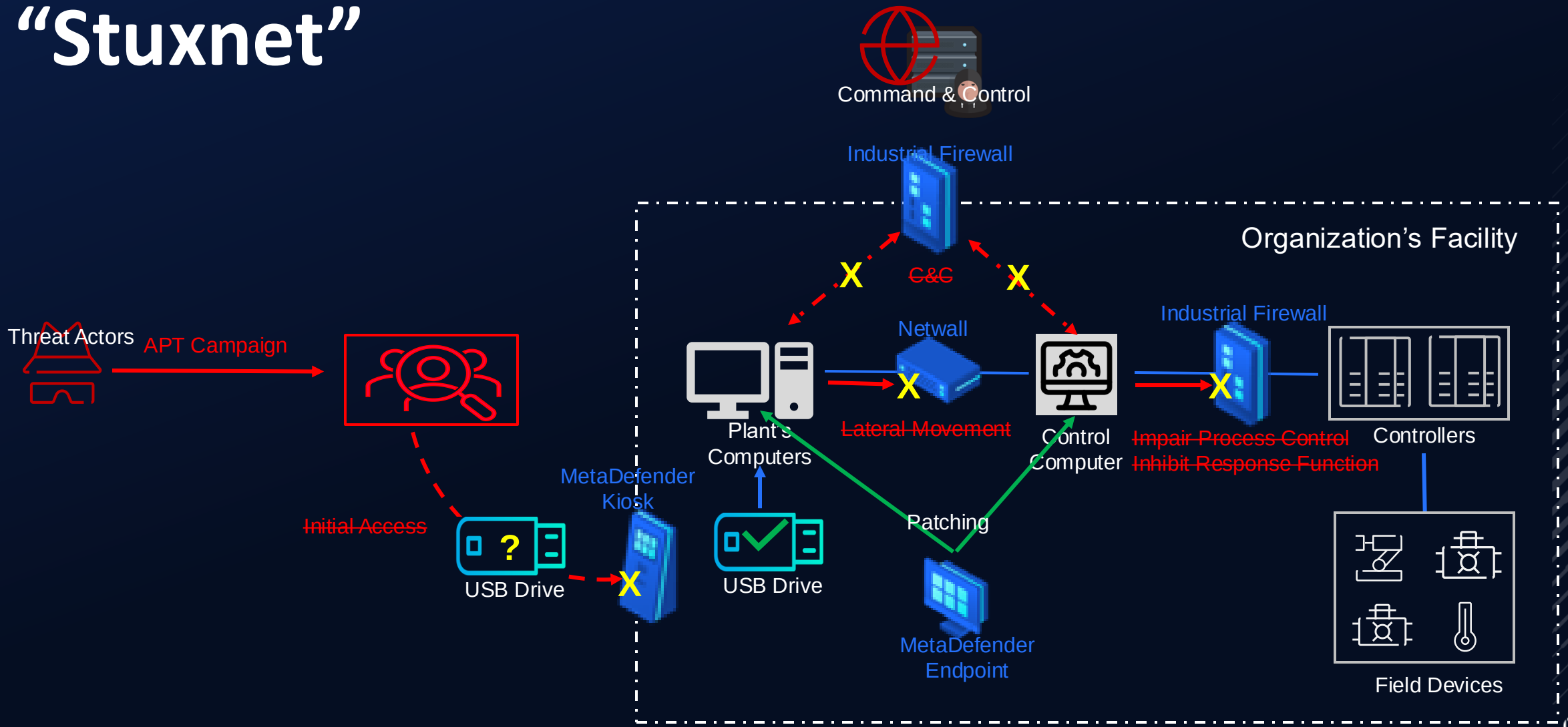
OPSWAT SOLUTIONS

Prevent “Stuxnet”



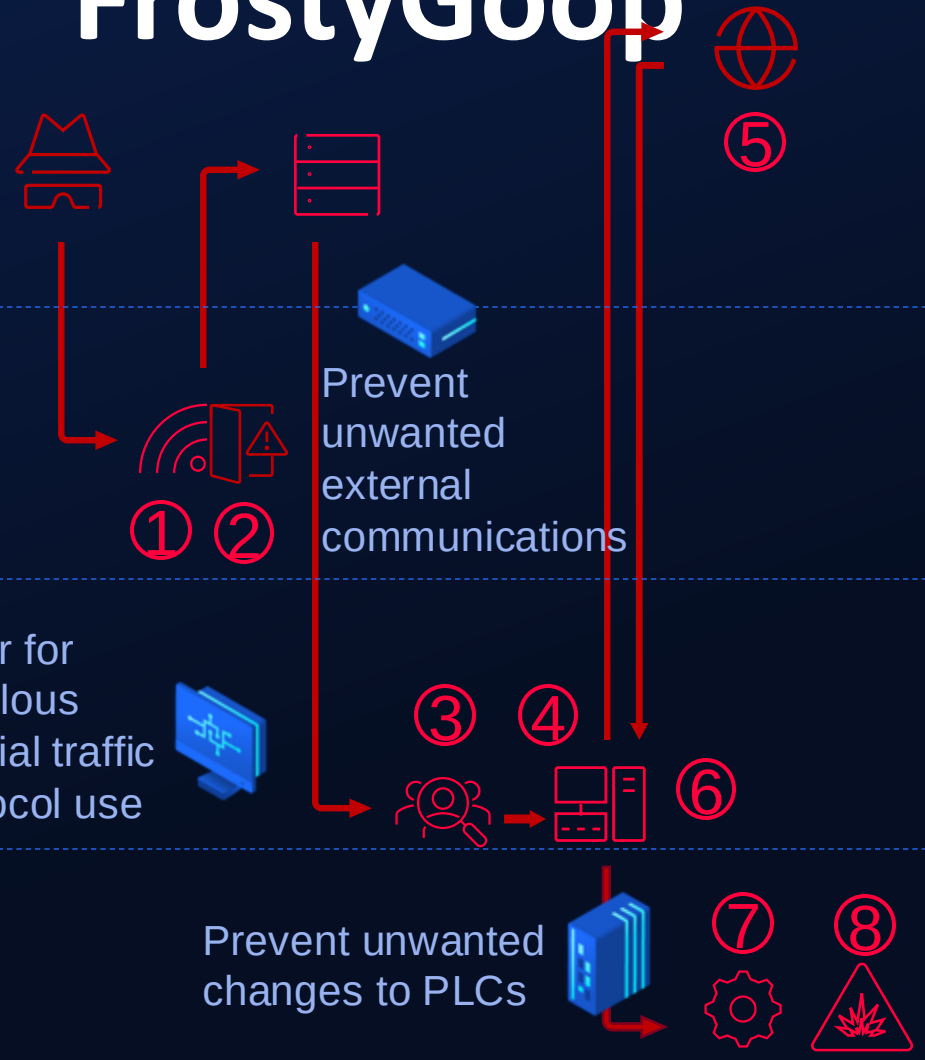
OPSWAT SOLUTIONS

Prevent “Stuxnet”

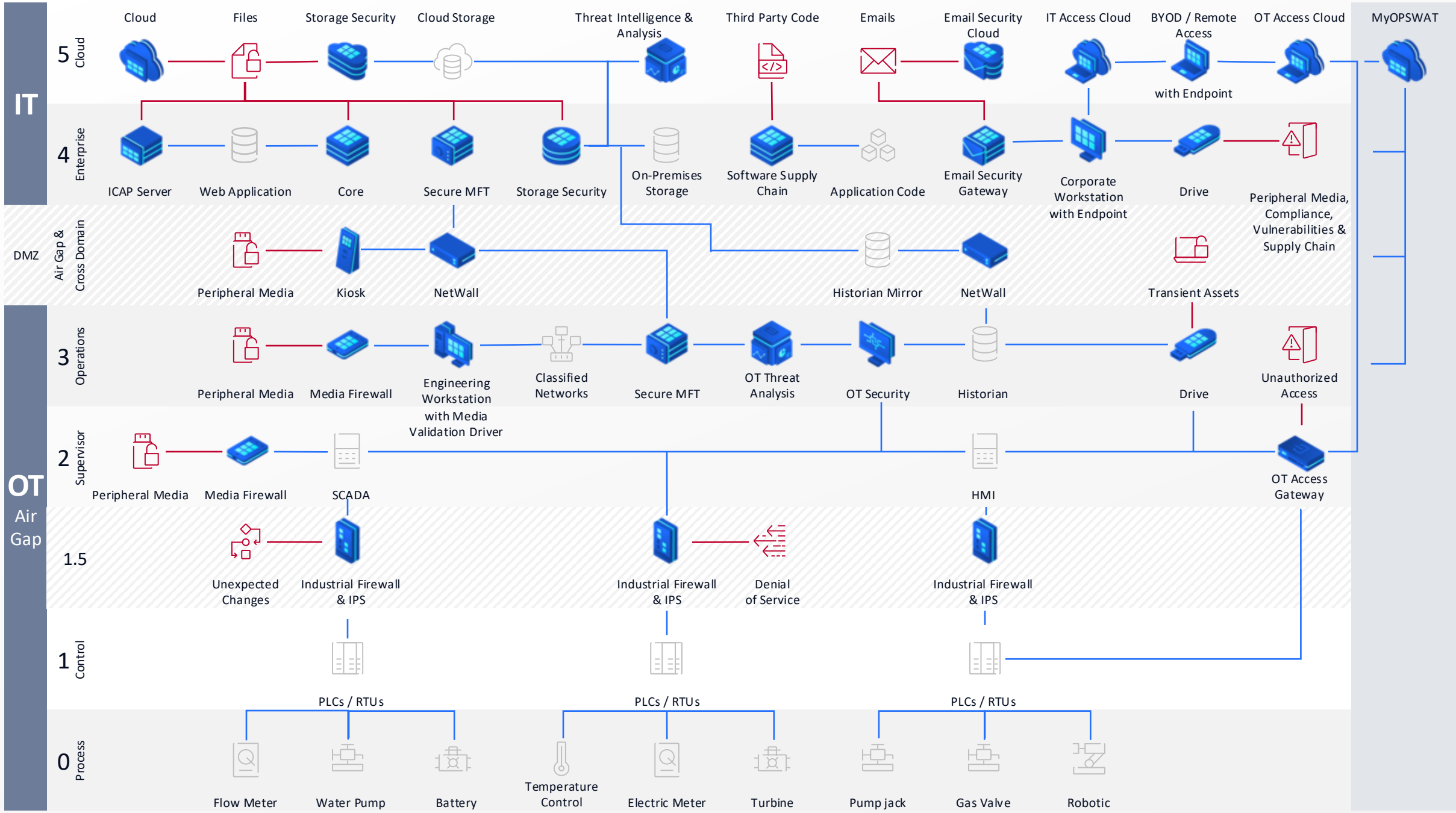


OPSWAT SOLUTIONS

Prevent “FrostyGoop”



1. ~~Threat actors exploit a vulnerability in external facing MikroTik router~~
2. ~~Deploy a webshell with tunneling accessed by a TOR Address~~
3. ~~Retrieve Security Account Manager (SAM) registry hive~~
4. ~~Deploy and test FrostyGoop Malware (Golang binary using JSON configs)~~
5. ~~Threat Actors establish connection to Moscow Based IP Addresses~~
6. ~~Threat Actors send malicious Modbus commands to FrostyGoop~~
7. ~~Commands are sent directly to the heating system controllers, reporting false measurements~~
8. ~~Process disables heat based on faulty measurements~~


IT
OT
Air Gap
DMZ
Air Gap & Cross Domain
5 Cloud
4 Enterprise
3 Operations
2 Supervisor
1.5
1 Control
0 Process
Cloud
Files
Storage Security
Cloud Storage
Threat Intelligence & Analysis
Third Party Code
Emails
Email Security Cloud
IT Access Cloud
BYOD / Remote Access with Endpoint
OT Access Cloud
MyOPSWAT
ICAP Server
Web Application
Core
Secure MFT
Storage Security
On-Premises Storage
Software Supply Chain
Application Code
Email Security Gateway
Corporate Workstation with Endpoint
Drive
Peripheral Media, Compliance, Vulnerabilities & Supply Chain
Peripheral Media
Kiosk
NetWall
Historian Mirror
NetWall
Transient Assets
Peripheral Media
Media Firewall
Engineering Workstation with Media Validation Driver
Classified Networks
Secure MFT
OT Threat Analysis
OT Security
Historian
Drive
Unauthorized Access
Peripheral Media
Media Firewall
SCADA
HMI
OT Access Gateway
Unexpected Changes
Industrial Firewall & IPS
Industrial Firewall & IPS
Denial of Service
Industrial Firewall & IPS
PLCs / RTUs
PLCs / RTUs
PLCs / RTUs
Flow Meter
Water Pump
Battery
Temperature Control
Electric Meter
Turbine
Pump jack
Gas Valve
Robotic

OUR VISION

We secure our way of life.

OPSWAT.




OPSWAT Vietnam

- Leading Global R&D Centre of OPSWAT, 400 R&D Engineers
- Offices in Ho Chi Minh and Hanoi City
- “Best Company to work for in ASIA Award” in 5 successive years

Visit us
Booth #9

OPSWAT.

Thank You!