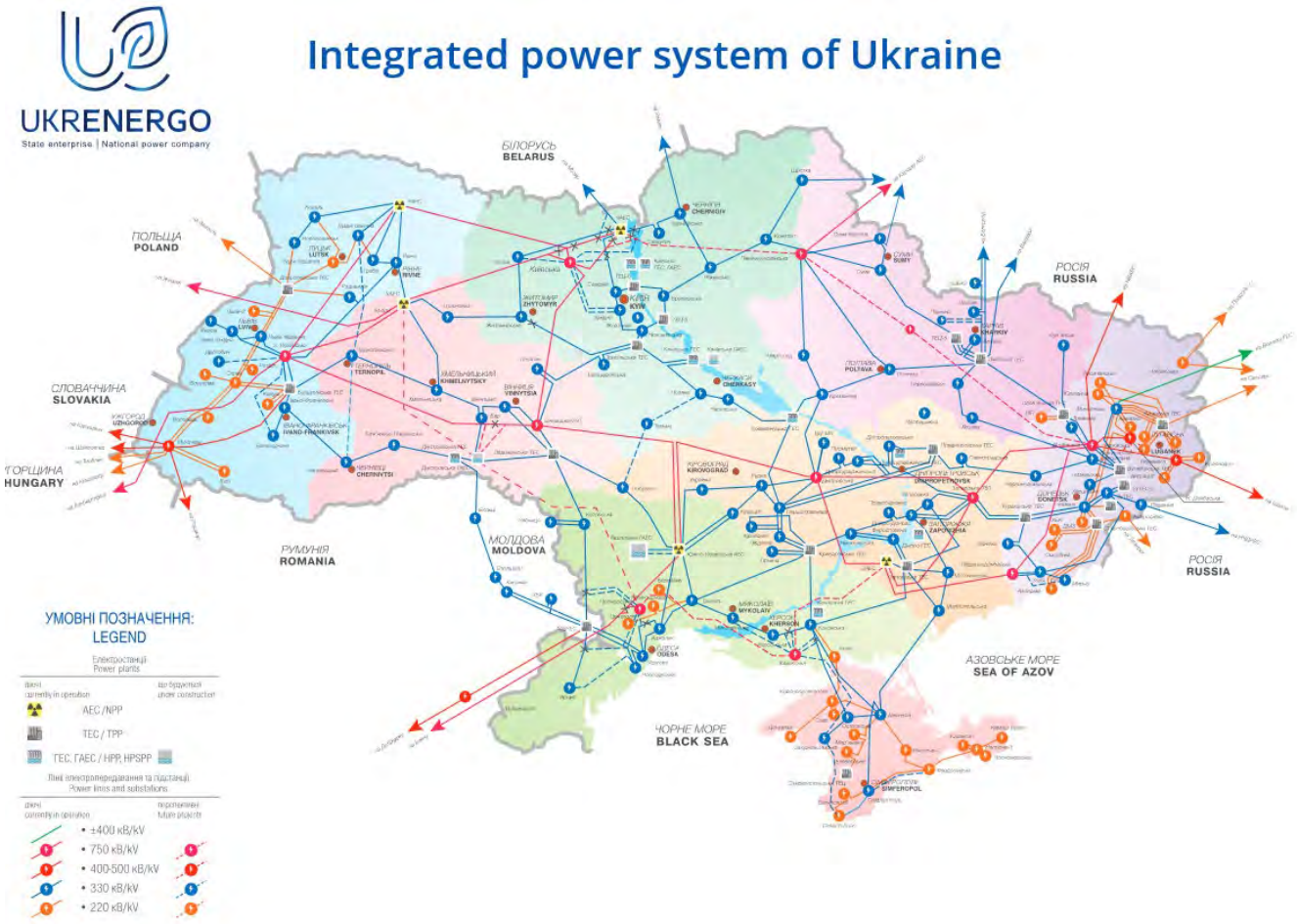
UKRENERGO
State enterprise | National power company



National Power Company UKRENERGO –

is a transmission system operator (TSO), which is responsible for electricity transmission from generating plants to DSOs.

UKRENERGO
State enterprise | National power company

One of our strategic goals and the main reason why we are under cyber attacks:

Ensure stable and balanced operation of the Integrated Power System of Ukraine

“Set up remote control at each substation until 2028” – is another ambition goal for transmission grid’s modernization and great challenge for our cybersecurity.

CRITICAL INFRASTRUCTURE is always a target for attack

UKRENERGO
State enterprise | National power company

The most famous cyberattacks against Ukraine's energy sector:

- **December 2015 – BlackEnergy.** The first large scale cyberattack on a power grid against three DSOs.

UKRENERGO
State enterprise | National power company

The most famous cyberattacks against Ukraine's energy sector:

- **December 2016 – Industroyer/Crash Override.** It was the cyberattack on one of the UKRENERGO`s substation.


ANDY GREENBERG SECURITY 06.12.2017 08:00 AM

'Crash Override': The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

UKRENERGO
State enterprise | National power company

The most famous cyberattacks against Ukraine's energy sector:

In August 2019 Dragos Inc published a detailed report about Industroyer/Crash Override. They say that hackers intended not merely to cause a short-lived disruption of the Ukrainian grid but to inflict lasting damage that could have led to power outages for weeks or even months. Idea was to cause physical damage to substation primary equipment.

ANDY GREENBERG SECURITY 09.12.2019 11:55 AM

New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction

A fresh look at the 2016 blackout in Ukraine suggests that the cyberattack behind it was intended to cause far more damage.

https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

UKRENERGO
State enterprise | National power company

The most famous cybe attacks against Ukraine's energy sector:

- **June 2017 – NotPetya.** The target of this attack was Ukraine, but whole world have been affected**.**
- Global damage worldwide was about $10 billions.


ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

'NotPetya' ransomware hits '2,000 organisations' in WannaCry-style global outbreak

Attack uses multiple vectors, including NSA exploit EternalBlue


BBC Sign in News Sport Reel Worklife Travel Future

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Politics Parliaments Brexit

UK and US blame Russia for 'malicious' NotPetya cyber-attack

15 February 2018 Share

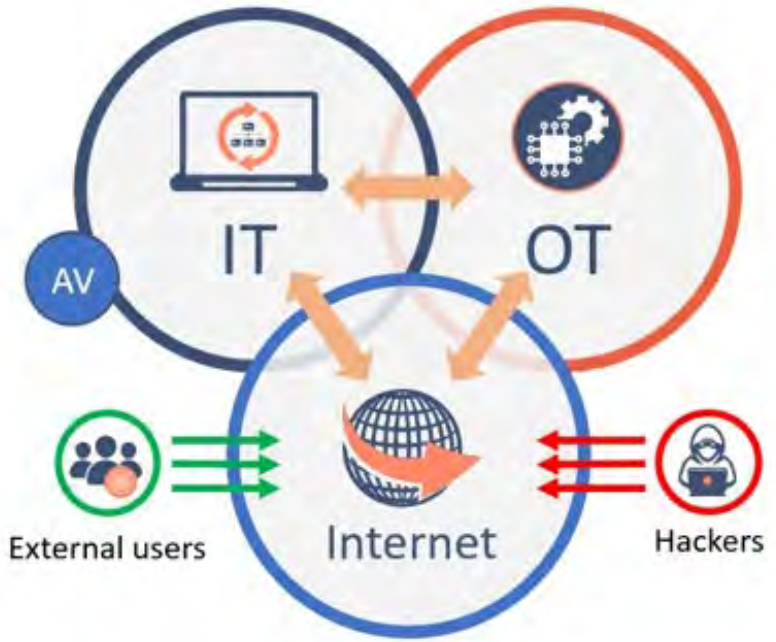
UKRENERGO
State enterprise | National power company

Why it became possible?

UKRENERGO

THE STATE THAT WAS IN 2016:

- Intersection of IT and OT;
- Lack of updates on infrastructure elements;
- Usage of unsupported manufacturer systems;
- Lack of information security unit;
- Lack of work with users.



UKRENERGO
State enterprise | National power company

INFORMATION SECURITY RISKS

«STRATEGIC RISKS»

«OPERATIONAL RISKS»

UKRENERGO
State enterprise | National power company

The nature of the risk :

NO MANAGEMENT DOCUMENT / PROCESS

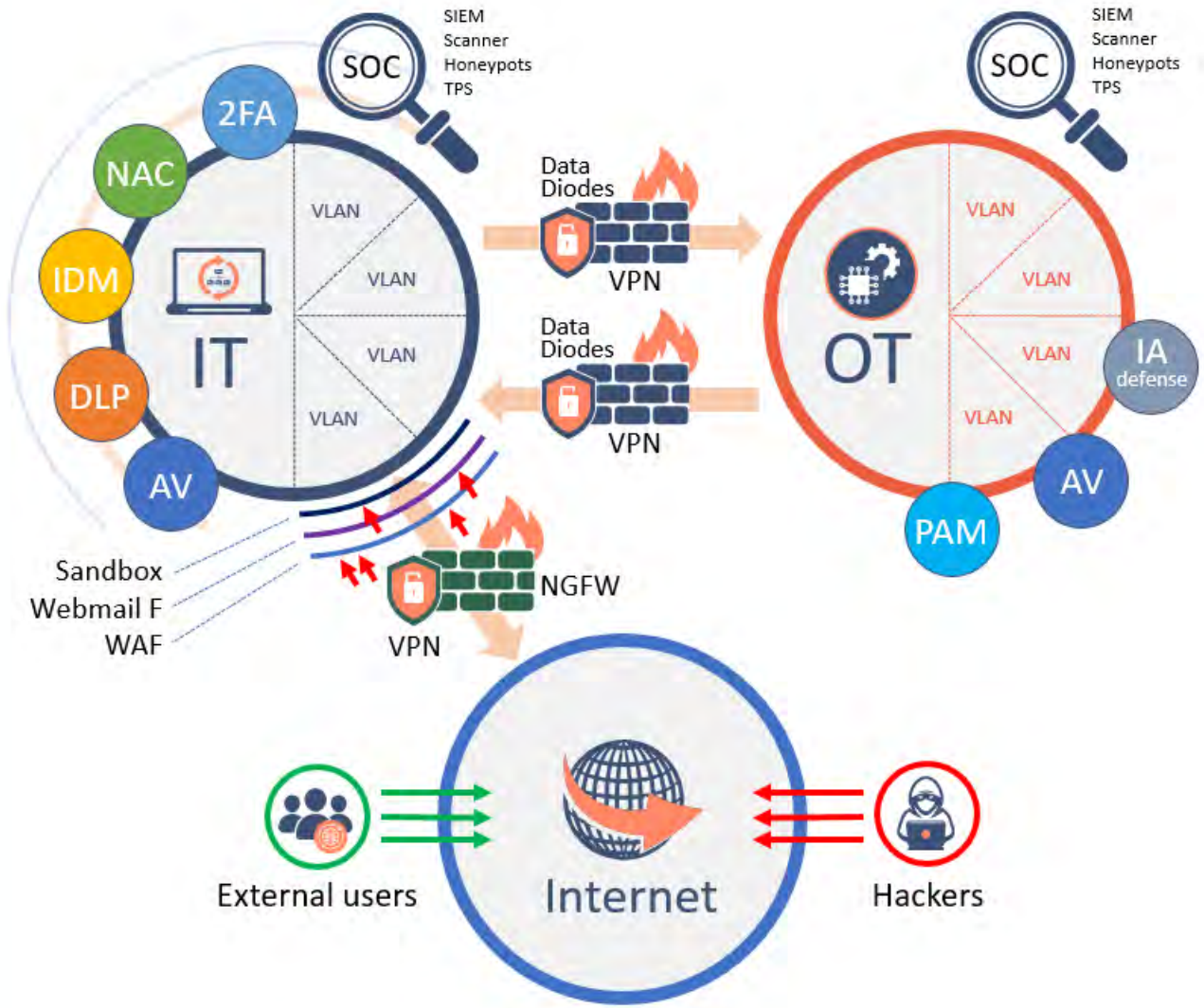
NO TECHNICAL SOLUTION

UKRENERGO
State enterprise | National power company

UKRENERGO
State enterprise | National power company

THE STATE THAT WILL BE ON 2019-2023

- Physical separation of IT and OT;
- Building a modern defense line;
- Monitoring and creation SOC;
- Starting the process of internal audits;
- Information security risk management.



UKRENERGO
State enterprise | National power company

OT SECURITY

UKRENERGO
State enterprise | National power company

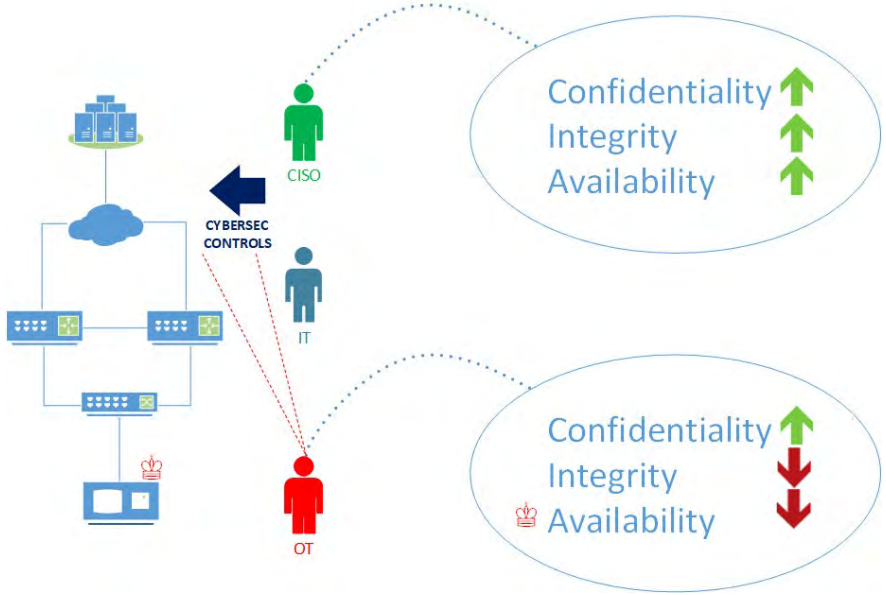
IT vs OT Security

Security Topic	Information Technology (IT)	Control Systems (ICS)
Anti-virus and Mobile Code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based	Memory requirements can impact on ICS; organizations can only protect legacy systems with after-market solutions; usually requires "exclusion" folders to avoid programs quarantining critical files
Patch Management	Easily defined; enterprise-wide; remote and automated	Long timeline to successful patch installation; OEM-specific; may "break" ICS functionality; asset owners required to define acceptable risk
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; usually same vendor over time; product end-of-life creates new security concerns
Testing and Audit Methods	Use modern methods; systems usually resilient and robust to handle assessment methods	Tune testing to the system; modern methods can be inappropriate; equipment may be susceptible to failure during testing
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact on production
Asset Classification	Common and performed annually; results drive expenditure	Only performed when obligated; accurate inventories uncommon for nonvital assets; disconnect between asset value and appropriate countermeasures
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Focused on system resumption activities; forensics procedures immature (beyond event re-creation); requires good IT/ICS relationships
Physical and Environmental Security	Can range from poor (office systems to excellent (critical IT operations systems)	Usually excellent for critical areas, maturity varies for site facilities based on criticality/culture
Secure Systems Development	Integral part of development process	Historically not an integral part of development process; vendors are maturing but at slower rate than IT; core/flagship ICS solutions difficult to retrofit with security
Security Compliance	Definitive regulatory oversight depending on sector (and not all sectors)	Specific regulatory guidance depending on sector (and not all sectors)

Source: https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP

Challenges

- Convergence between IT and OT networks
- Lack of visibility of the OT network
- Old, unsecured and non-standard protocols
- Legacy Software/Firmware/ Hardware



Cyberbit SCADAShield

Cyberbit SCADAShield is a non-intrusive solution for OT network monitoring, detection, forensics and response. It discovers and visualizes all OT network components and communications, monitors both OT and IT protocols, and enables OT and IT managers to detect, analyze and respond to network anomalies, vulnerabilities and threats.

https://www.cyberbit.com/solutions/ics-scada-security-continuity/

UKRENERGO
State enterprise | National power company

The CyberX Platform

The CyberX platform delivers continuous ICS threat monitoring and asset discovery, combining a deep embedded understanding of industrial protocols, devices, and applications with ICS-specific behavioral anomaly detection, threat intelligence, risk analytics, and automated threat modeling.

https://cyberx-labs.com/

UKRENERGO
State enterprise | National power company

The Dragos Platform

The Dragos Platform is industrial cybersecurity software codified by ICS practitioners that passively identifies ICS network assets, pinpoints malicious activity, and provides step-by-step guidance to investigate incidents and respond.

https://dragos.com

UKRENERGO
State enterprise | National power company

The Indegy Industrial Cybersecurity Suite

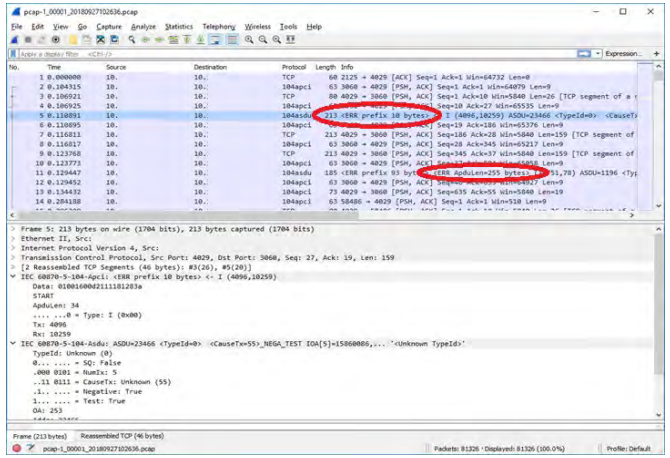
The Indegy Industrial Cybersecurity Suite protects industrial networks from cyber threats, malicious insiders, and human error.

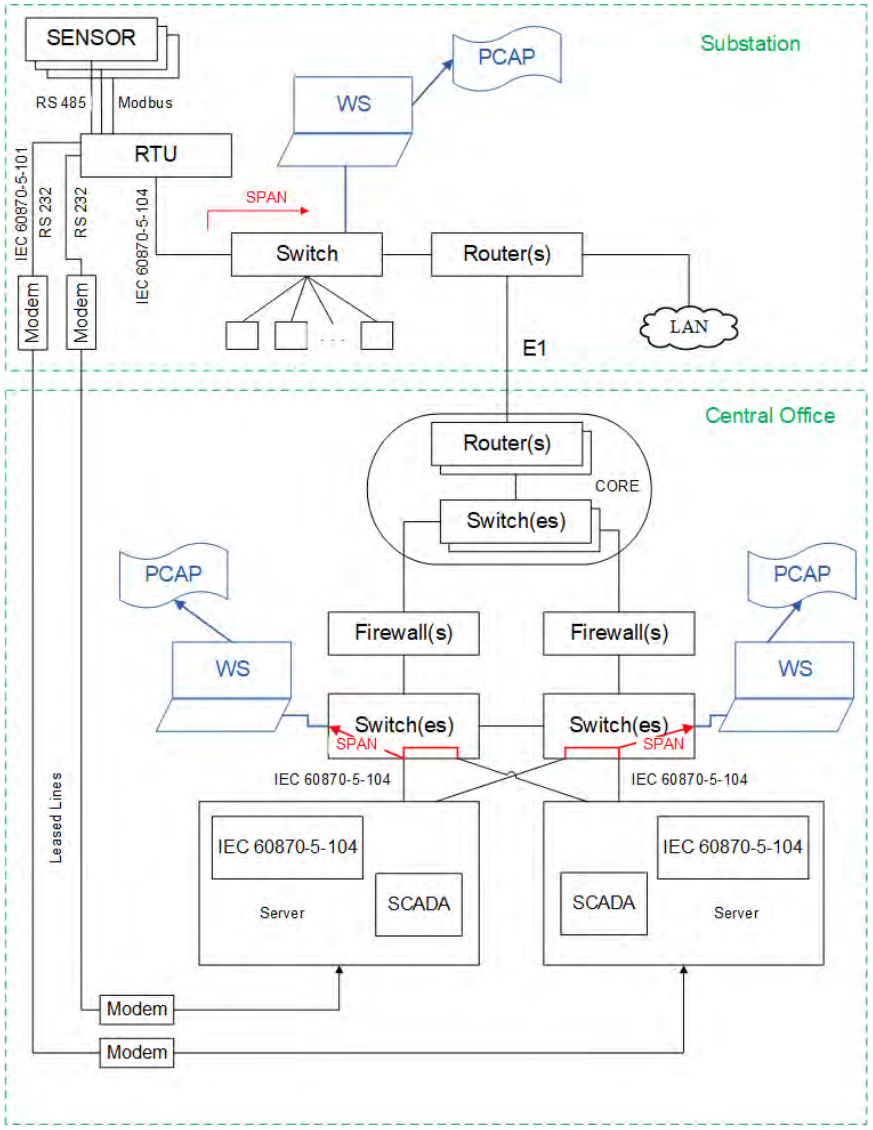
https://www.indegy.com

UKRENERGO
State enterprise | National power company

Preparing for tests

- NDA
- Test scope (OT/IT)
- Network architecture for tests
- PCAPs
- Non-standard protocols (modified IEC 60870-5-104)
- Non-standard ports for OT protocols (<> 2404/tcp)

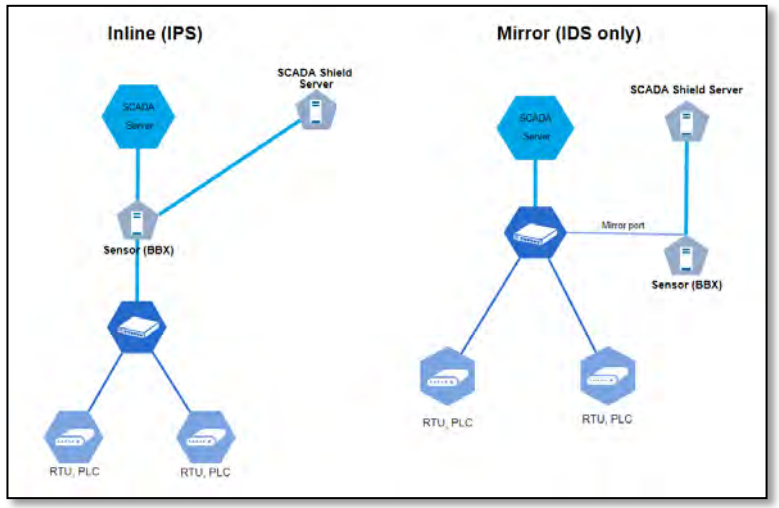


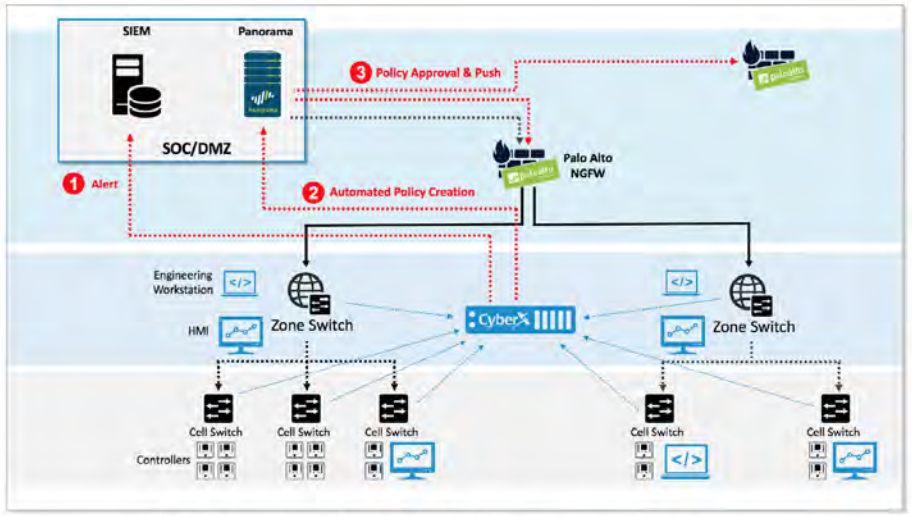


UKRENERGO
State enterprise | National power company

IPS

- Inline mode
- Integration with firewalls



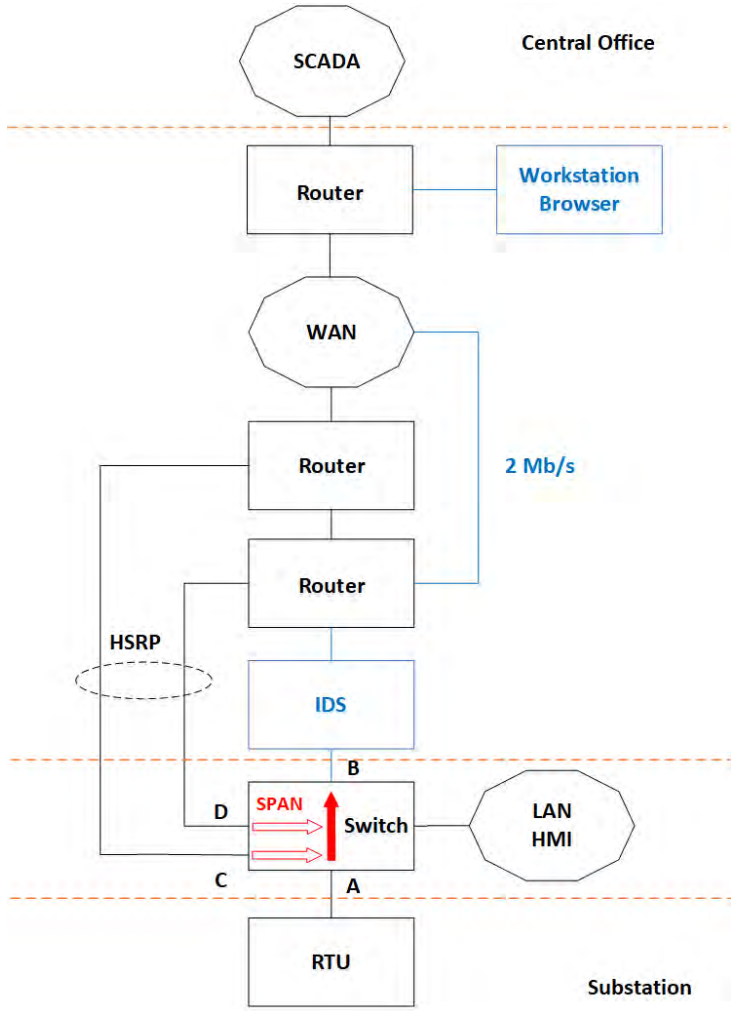


CyberX's integration with Panorama™ enables joint customers to rapidly block sources of malicious traffic in ICS/SCADA networks

Testing Stages

Network-based Behavioral Anomaly Detection (BAD)

- Learning mode
- Baseline
- Production mode

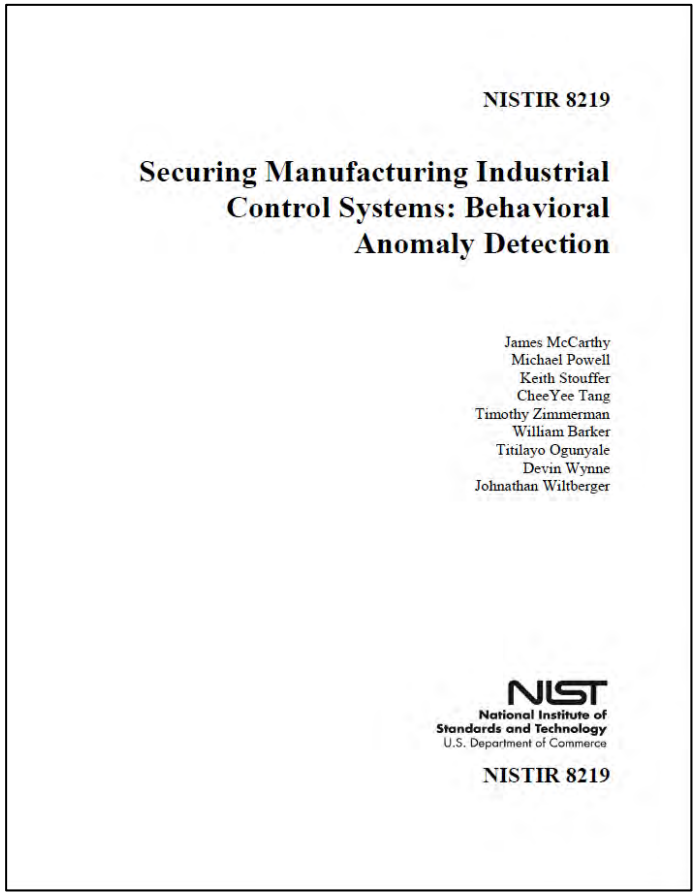


UKRENERGO
State enterprise | National power company

Benefits

1. Discover, map and control all your industrial network assets
2. Visualize your entire network and identify changes
3. Monitor your network and receive real-time alerts on suspicious activity
4. Track unauthorized devices, communications and actions
5. Identify known CVEs and alert upon detection
6. Mitigate equipment and protocol vulnerabilities, exploits and security issues
7. Conduct forensics and investigations and analyze root cause
8. Customize dashboards and reports easily and quickly

Additional Reading



NISTIR 8219 (DRAFT)

This report is intended for individuals or entities that are interested in understanding behavioral anomaly detection (BAD) technologies and their application to ICS environments. Additionally, this report is intended for those who are interested in understanding how to implement BAD tools in ICS and other operational technology environments.

https://csrc.nist.gov/publications/detail/nistir/8219/draft

Additional Reading

CyberX's 2019 GLOBAL ICS & IIOT RISK REPORT

A data-driven analysis of real-world vulnerabilities observed in more than 850 production ICS networks across all industrial sectors and 6 continents

https://cyberx-labs.com/resources/risk-report-2019

UKRENERGO
State enterprise | National power company

Thank you for your attention!

Taras Vasyliv
SSCP, Head of Dispatching Control System Department
NPC UKRENERGO

Andrii Chubyk
Leading Analyst Analytics and International Studies Division
NPC UKRENERGO