LIVE WEBINAR

PRESENTED BY: Utilities Technology Council

Navigating RegulatoryCompliance Mandates for Utilities Cybersecurity

Brian Tolly
Director, Network Test & Visibility
Tempest

Patrick Miller
CEO
Ampere Industrial Security

Eric Floyd
Director, Industrial Soutions
Keysight Technologies

Compliance landscape

- NERC CIP
- TSA Pipeline Safety Guidelines & Security Directives
- API 1164
- Executive Orders
- National Security Memorandum
- NIST 800-53/800-82
- Controls vs. Performance
- Good Evidence Practices

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Crystal ball

- Each “catalytic event” creates a cyber-avalanche
- NERC CIP moved the needle for electric sector, everyone noticed
- Legislators, regulators and commissions are educated and aware
  - 18 new cybersecurity bills introduced in the last session
  - On pace for even more this session
- Regulation is always considered as a response
- So many federal motions in so many government and industry verticals it’s hard to understand them all…

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Biden 100-day Plan Plan to Address Cybersecurity Risks to the U.S. Electric System

100-day Plan for electricity ss

The initiative modernizes cybersecurity defenses and:

- Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities
- Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
- Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks; and
- Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

100-day plan for Electricity ss

- Internal network anomaly detection
- External network anomaly detection
  - CRISP, Neighborhood Keeper, Essence
- Boundary level detection
  - UTM, firewall, NIDS
- System level detection
  - Tripwire (integrity monitoring)
  - HIDS
  - Antivirus
  - Application whitelisting
- SOC/SIEM capacity
- Information Sharing…
- 100 days has already passed with no public release from ESSC

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

National Security Memorandum

- Not a law/regulation – voluntary collaborative initiative (for now)
- Baseline security controls across all critical infra sectors
- Some controls will be common with existing frameworks (CIP)
- NIST 800-53/82 are being promoted (expected) to be the set
- Measurement (no enforcement) will be DHS CISA and SSA
- Unclear how measurement will happen (audit, assessment?)
- Will apply first to electricity subsector, then gas, chemical, water
  - Unclear if “National Security” banner will loop in Distribution
- Final framework to be completed by July 28, 2022
- Clear signaling that participation is expected, or else…

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

NSM – What do I need to do?

- "…deployment of technologies and systems that provide threat [and anomaly] visibility, indications, detection, and warnings…"
- "…response capabilities for cybersecurity in essential control system and operational technology networks…"
- …" Government and industry to collaborate to take immediate action…"
- "…baseline cybersecurity goals that are consistent across all critical infrastructure sectors…"

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

NSM – Recommended Actions

- Gap assessment of current CIP controls against 800-53/82
  - CIP has already been mapped, use existing tools
- Create action plan to remediate any control gaps
  - Owners, actions, dates, budget
- Begin any architecture/system modifications needed for increased monitoring, detection, response and recovery
- Procure and/or tune network anomaly detection software
  - CRISP, Neighborhood Keeper, Essence or other commercial tool
- Establish trained and resourced security operations function
  - Can be outsourced or insourced
  - Process, analyze, respond and tune new tools
- Perform REAL incident and recovery response exercises

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

NSM – voluntary vs. mandatory

- PR incentives/hit – public perception minimum bar has been set
- Cyber insurance impacts can be very real
- Business partnerships – upstream/downstream; M&A, contracts
- Constrained markets over time
- Earlier adopter bonus points with oversight body
- Easier to demonstrate proactive continuous improvement vs. late-stage, time-constrained, forced, and reactive efforts
- Given the situational gravity, it may be inevitable
- If not the NSM, then any one of the other “influences”

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Direct signaling

"...defend US critical infrastructure by encouraging & facilitating deployment of tech & systems that provide threat visibility, indications, detection, & warnings, & that facilitate response capabilities for cybersecurity in essential control system & operational tech networks."

"We're committed to addressing it. We're starting with voluntary, as much as we can, because we want to do this in full partnership. And — but we're also pursuing all options we have in order to make the rapid progress we need."

"...multiple administrations have recognized that there are no mandated authorities to mandate cybersecurity requirements for critical infrastructure... in the context of our openly saying that we really are committed to addressing the limited and piecemeal regulation..."

"The President is essentially saying, 'We expect responsible owners and operators to meet these performance goals. We will look to you to implement this.'"

- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, The White House

June 28, 2021

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Relevant Executive Orders

Executive order 13873

“Securing the Information and Communications Technology and Services Supply Chain"

- Issued by Trump, May 15 2019
- Unprecedented authority to prevent or modify transactions involving information and communications technology and services (“ICTS”) originating in countries designated as “foreign adversaries” which pose an undue risk to critical infrastructure or the digital economy in the United States, or an unacceptable risk to US national security

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Executive order 13920

“Securing the United States Bulk-Power System”

- Issued by Trump, May 1 2020
- Declared a National Emergency for BPS
- Issued a Prohibition Order; primarily a supply chain motion
- No-buy list of countries and vendors
- Task force on Federal Energy Infrastructure Procurement Policies Related to National Security
- Pre-approved list of countries and vendors
- Paused for 90 days by Biden on Jan 20, 2021
- Biden Admin revoked the Prohibition Order on April 20, 2021

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Executive order 14017

“America’s Supply Chains”

- Issued by Biden February 24, 2021
- Wide-ranging evaluation of America’s supply chains over 1 year with two tracks:
- 100-day review
  - semiconductors and advanced packaging;
  - high-capacity batteries;
  - critical minerals and other identified strategic materials; and
  - active pharmaceutical ingredients
- Year long review
  - defense industrial base;
  - public health and biological preparedness industrial base;
  - information and communications technology (ICT) industrial base;
  - energy sector industrial base;
  - transportation industrial base;
  - agricultural commodities and food products

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Executive order 14028

“Improving the Nation's Cybersecurity”

- Issued by Biden, May 12, 2021
- Remove barriers to threat information sharing between government and the private sector
- Modernize and implement stronger cybersecurity standards in the federal government
- Improve software supply chain security
- Establish a cybersecurity safety review board (Cyber NTSB)
- Create a standard playbook for responding to cyber incidents
- Improve detection of cybersecurity incidents on federal government networks
- Improve investigative and remediation capabilities
- Labeling programs related to the Internet of Things (IoT) and software to inform consumers

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

TSA Pipeline Safety Guidelines and Security Directives

TSA Pipeline Security directive #1

- May 27, 2021 – Security Directive-Pipeline-2021-01
- Within 30 calendar days, conduct a detailed gap assessment of their cybersecurity programs using the TSA's Guidelines; remediation measures
- Report information and physical security incidents affecting their IT or operational technology OT systems to CISA within 12 hours of identification. Reportable incidents include:
  - Unauthorized access;
  - Discovery of malicious software;
  - Denial of service (DoS) attacks;
  - Physical attacks against network infrastructure; and
  - Any other cybersecurity incident that disrupts systems or facilities, "or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety" or have the potential to disrupt system or facility operations
- Designate a Cybersecurity Coordinator

TSA Pipeline security directive #2

- **Known:**
  - Implement specific mitigation measures to protect against ransomware attacks and other known threats to IT & OT
  - Develop and implement a cybersecurity contingency and recovery plan
  - Conduct a cybersecurity architecture design review
- **Reported/rumored:**
  - Password updates
  - Disabling Microsoft macros
  - Programmable logic controller (PLCs) protections
  - Antivirus/malware protection
  - Detection technologies
  - Ingress and egress communications
  - System segmentation
  - Multi-factor authentication (MFA)
  - Zero trust

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Direct Signaling

"For over a decade, the Federal Energy Regulatory Commission (FERC), in coordination with the North American Electric Reliability Corporation, has established and enforced mandatory cybersecurity standards for the bulk electric system. However, there are no comparable mandatory standards for the nearly 3 million miles of natural gas, oil, and hazardous liquid pipelines that traverse the United States.

"It is time to establish mandatory pipeline cybersecurity standards similar to those applicable to the electricity sector. Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors. Mandatory pipeline security standards are necessary to protect the infrastructure on which we all depend.

"Therefore, I am pleased that Commissioner Clements is joining me today in my longstanding calls for mandatory cybersecurity standards for our nation's pipeline infrastructure."

- FERC Chairman Richard Glick, May 10, 2021

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE


NERC CIP Horizon

NERC CIP crystal ball

- Legislators, regulators and agencies are getting wiser
- Drifting toward NIST (FERC RFI)
- Focus on CIP-007, CIP-008 and CIP-009
  - Monitoring, incident response, and recovery
- Supply Chain
  - Coming to a Low Impact asset near you
- Cloud (BCSI and BCS)
- Virtualization
  - Biggest shift in CIP since v3 to v5
- Global adoption is picking up steam

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE


Common Threads

Regulatory landscape

- Global trend…
  - NIS, CAF, BSI, 62443, NIST 800-53/82/CSF, NERC CIP and many more
- FERC RFI seeking to align with NIST (and incentives)
- DOE RFI seeking information on possible additional security controls
- 100-day Plan to Address Cybersecurity Risks
- ES-C2M2 (new version) and ONG C2-M2
  - Both are being used by commissions and underwriters
- TSA Pipeline Security Guidelines updated, Security Directives (x2)
  - Possible addition of API 1164
- Recent updates to CFATS
- Too many Executive Orders to list
- New National Security Memorandum
- DHS CISA ICS attack history (posturing)
- Renewed interest in AWWA G430 and J100 standards

“Regulatory” Forecast

- Whether direct regulation (CIP, TSA, AWWA, CFATS) or indirect “transitive” regulation (NIST, EO, NSM), new normal is:
  - Buy only “trusted” hardware, software, services
  - Know all cyber assets in your environment
  - Know the security posture for all cyber assets
  - Segment and restrict access (zero trust, MFA)
  - Monitoring and detection at asset and network level
  - Strong incident response capability
  - Strong recovery capability
- Less “guessing” - aligns with guidelines, regulation, Executive Orders, National Security Memos, etc. in peer sectors
- Get ahead of this before it is mandated

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Assets and Architecture

- **Do you have an asset inventory?**
  - Not everything, but even just the critical stuff
  - Back it with change control or expect drift (waste time/money)
- **Do you have an environment you can defend?**
  - Segmented networks
  - One-way traffic
  - MFA and strict remote access controls
  - Shear-away networks, “crumple zones,” intelligent islanding
- **Interdependencies can be your Achilles heel**
  - Runs converse to many current approaches

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Situational awareness

- Would you know – with sufficient confidence – if there was (or was not) an adversary in your system?
- Monitoring is in every federal conversation now
  - CRISP, Neighborhood Keeper, Essense…
- "Smoke detectors" will be required in the "building code"
- Regulation, insurance, diligence, reporting (data breach)
- Start where you can, tune, then lather, rinse, repeat
- Based on solid asset inventory and feeds response and/or recovery

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Supply chain risk management

- NERC CIP-013 is the tip of the iceberg
  - Adding new asset types and moving to low impact
- Multiple Executive Orders, probably more to come
- ”No-buy” lists, rip/replace, legacy risk often unaddressed
- “Made in” often means “assembled in”
- How far do you go? Was it far enough?
- HBOM, SBOM, FBOM
- “CyberStar,” transparency centers, certification, validation
- Frustration and costs go up for everyone

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Practice like it's game day

- When was the last time you did a **real** incident response exercise?
  - Did it include a recovery drill?
  - Did it include IT impacting OT through business process?
- Everything else leads up to this
  - Asset inventory, supply chain, segmentation, monitoring
- Borrow from operations (and safety)
  - Can you really go to manual? For how long? 23A494
- Expect "oversight" and media when it happens
  - Cyber NTSB, CISA, E-ISAC, FBI, Commerce, State…
- What happens to one utility will affect all others…

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Common solutions

- For organizations already subject to NERC CIP, TSA, CFATS, AWWA, much can be borrowed
- Other controls frameworks also exist for an “overlay” (mapping) approach to managing compliance risk
  - Focus on NIST 800-53 and 800-82
- Portable skill sets across sector types in OT
  - IT already has common skill pool
- Some common solutions exist for IT and OT
  - Hardware
  - Software

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE

Controls vs. performance

- **How are you going to be measured?**
- **Performance**
  - Much less on the how, more on the what
  - Proof that you did what the requirement says
  - Very subjective
- **Controls**
  - Control objective defined, control designed, control test performed
  - Ensures all controls are functioning as expected
  - Preventive or detective
  - Procedural or technical
  - Much less subjective

Good evidence practices

- **Performance-based audits/assessments**
  - Policy, program, procedure, process stating “why” and “how”
  - At least one piece of evidence with proof requirement was performed
  - Word documents, Excel, PDF (everything else)
  - Consistency is very important
- **Controls-based audits/assessments**
  - Well-defined control objective that maps to existing standard/framework
    - What you are trying to control and why
  - Well-defined control that maps to existing standard/framework
    - How you are applying the control objective controlling the process/thing
  - Documented control test that demonstrates the control is functioning as expected

Keysight OT Security offerings

Complete validation of your OT environment

Pre-Production

Lab

Production

Visibility of existing OT network

Threat Simulation of existing and new OT network

(1) Validating SCADA Networks in a Lab environment

(2) ICS/OT Security Visibility

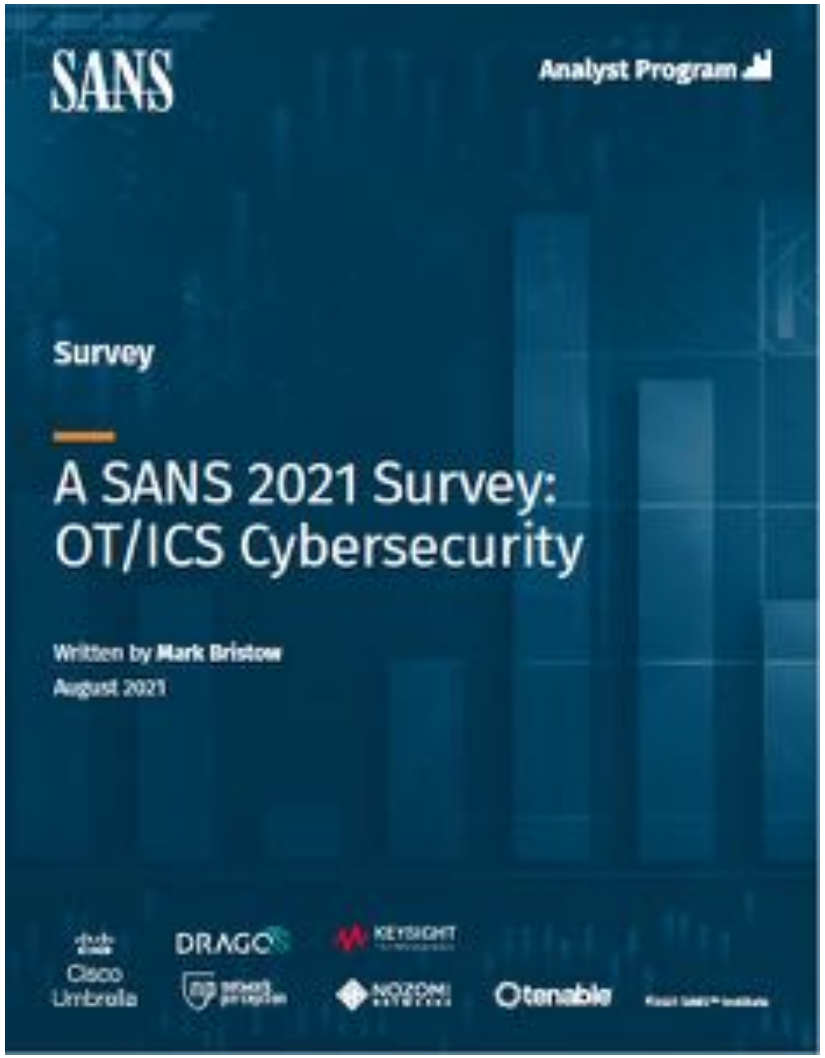
(3) Continuously monitor the efficacy of your network security controls.

TEMPEST TELECOM SOLUTIONS

KEYSIGHT TECHNOLOGIES

AMPERE

Industrial asset owners lack full security visibility



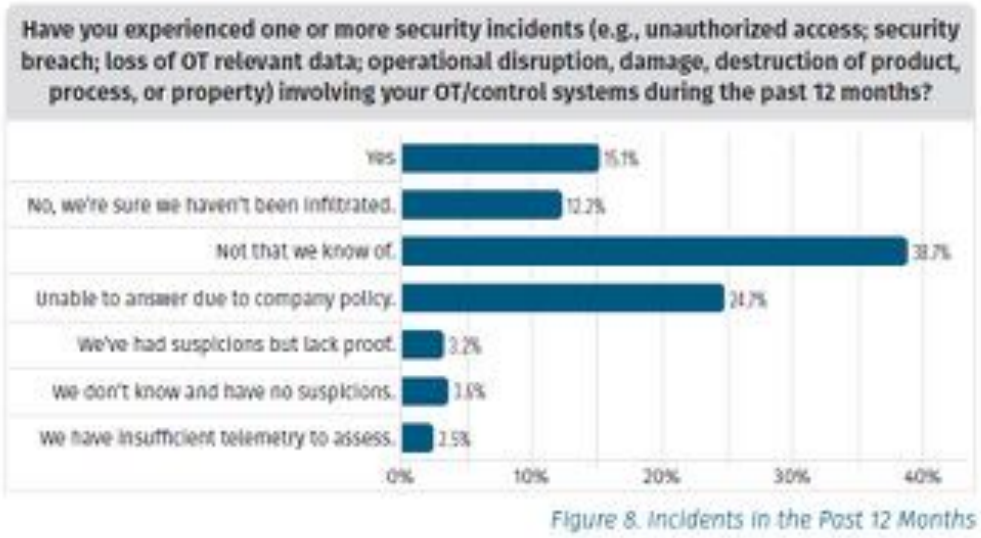
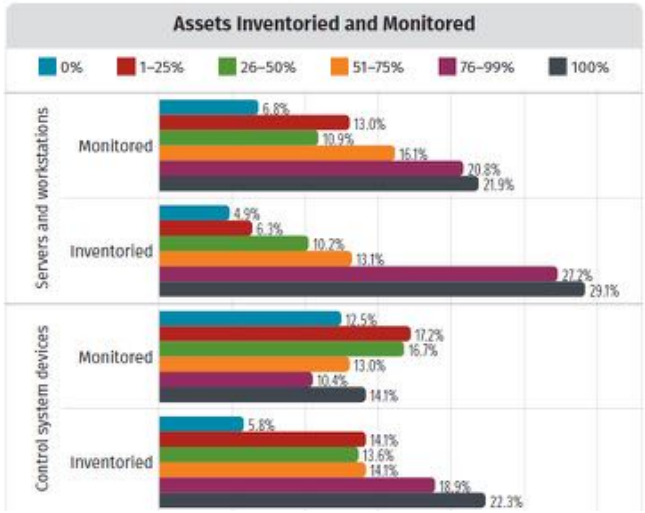


Figure 8. Incidents in the Post 12 Months



TEMPEST TELECOM SOLUTIONS

KEYSIGHT TECHNOLOGIES

AMPERE

Keysight Helps Provide Full Packet Visibility for NERC CIP Compliance

ROLE OF TAPS AND NETWORK PACKET BROKERS IN SUBSTATION

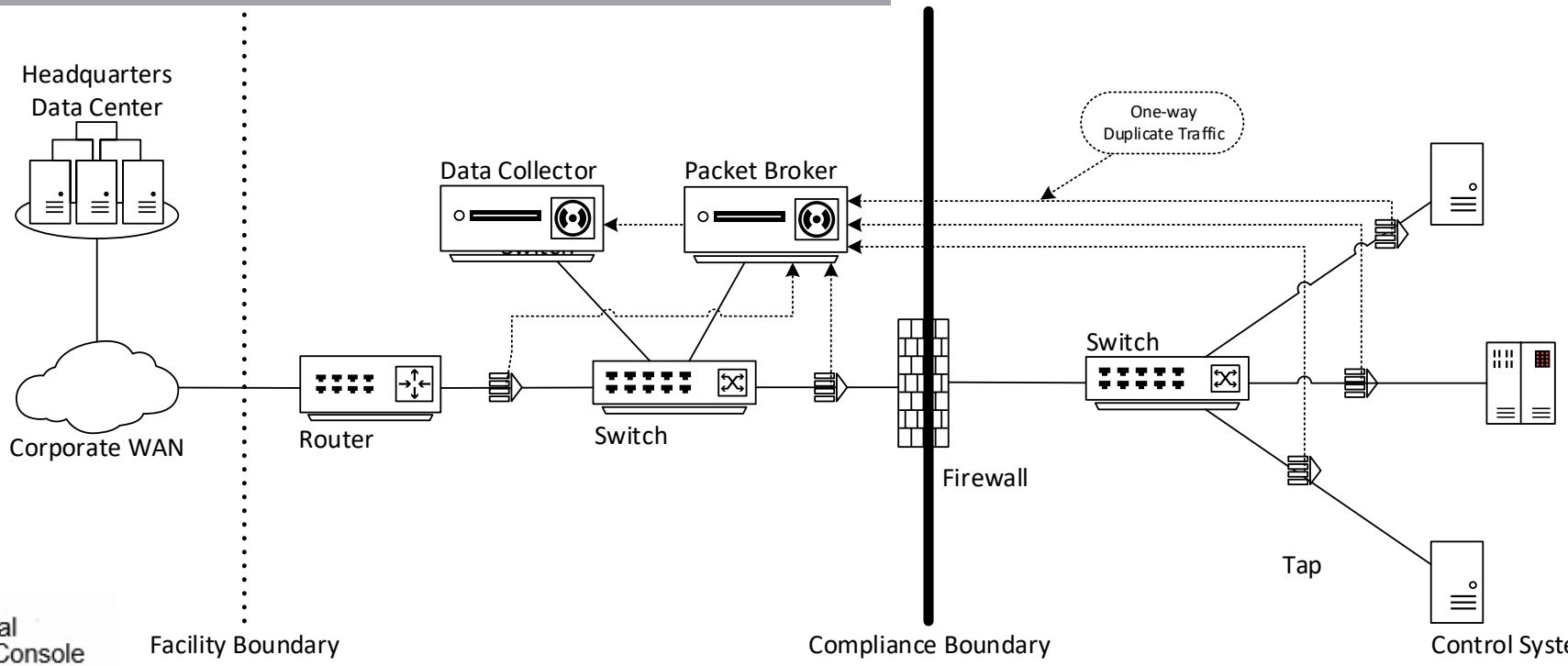
Industrial | ICS | OT | IOT

NOZOMI NETWORKS · FORESCOUT · armis · DRAGOS · CLAROTY · SCADAfence

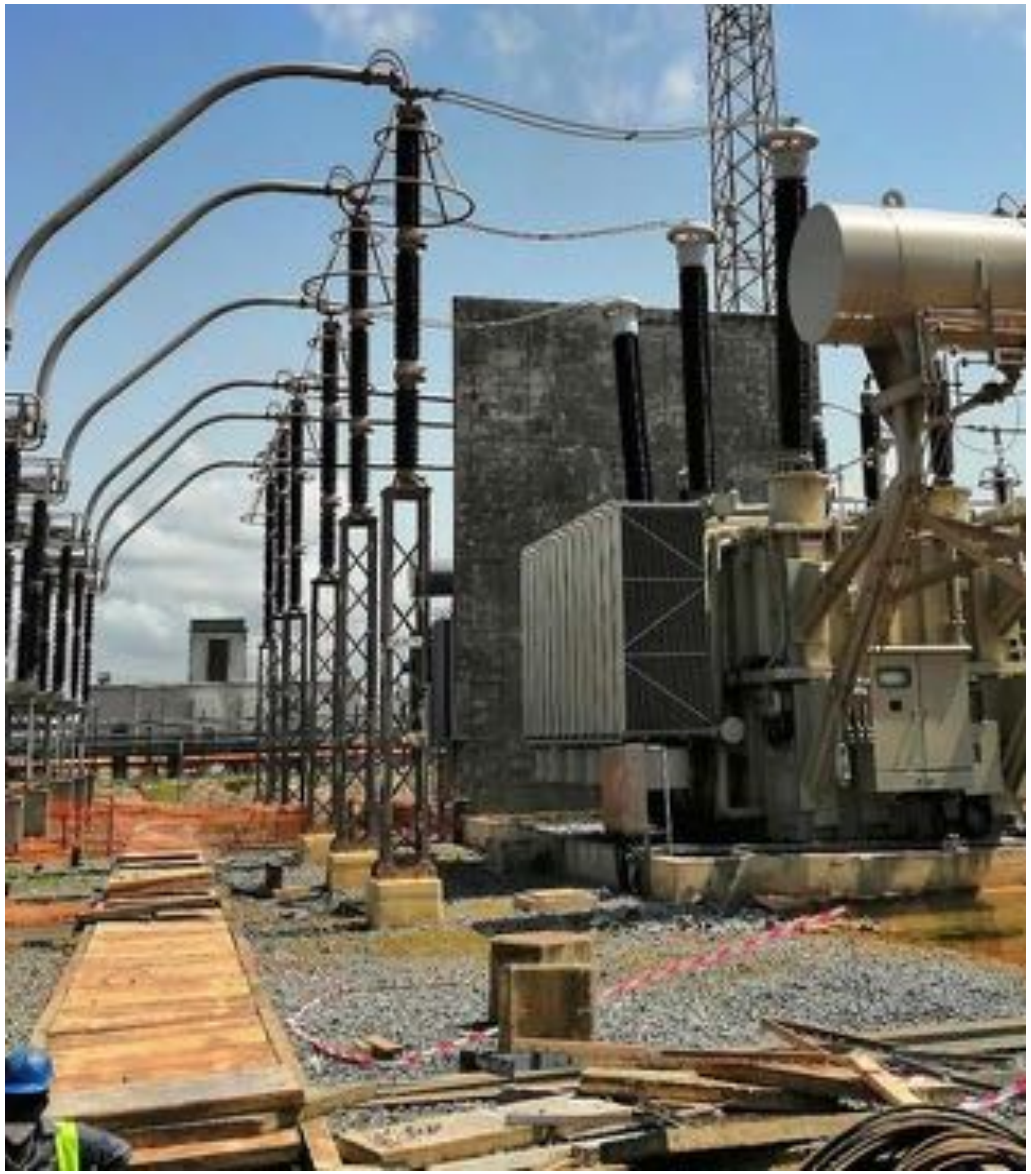
Identify – Asset Discovery and Network Visualization

Assess – Vulnerability Assessment and Risk Monitoring

Detect – Anomaly and Threat Detection

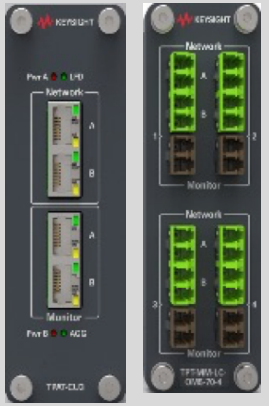


TEMPEST TELECOM SOLUTIONS · KEYSIGHT TECHNOLOGIES · AMPERE



Introducing Keysight's Tough Product Series

Industrial Network Packet Aggregator



Industrial Copper and Fiber taps

Power Supplies

TEMPEST TELECOM SOLUTIONS

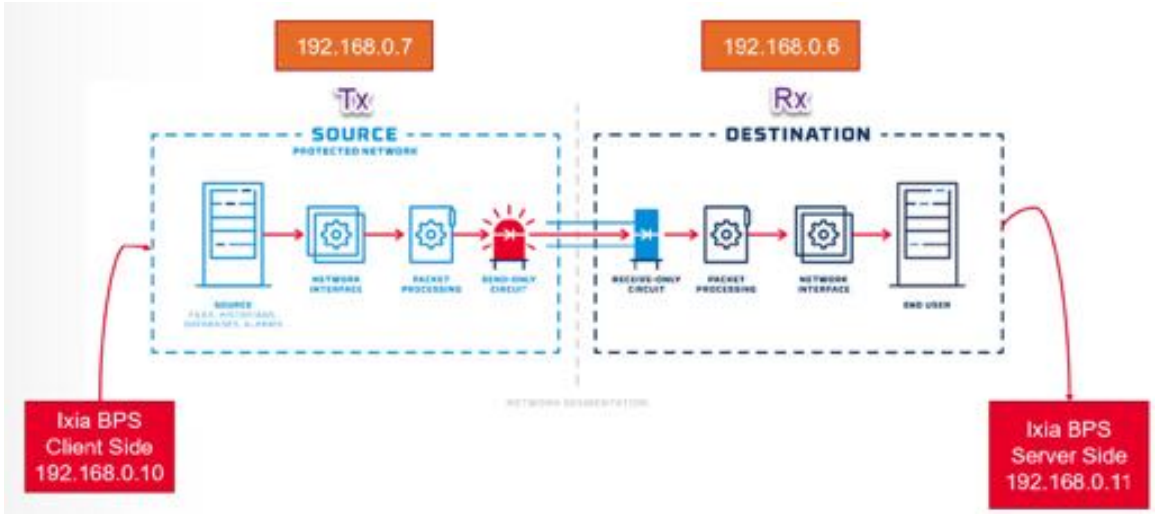
KEYSIGHT TECHNOLOGIES

AMPERE

Breaking Point Test Use case: Oil and Gas company

OT SECURITY – CHOOSING THE RIGHT DATA DIODE

- A Leader in Oil and Gas from Middle East, wanted to implement one of the key security procedures in their OT network: adding data diodes which allow traffic to flow only in one direction
  - One key element during FAT (Factory Acceptance Testing) was to ensure that the data diode was providing the required functionally: a vital cybersecurity solution that is used to protect isolated networks from cyber threats and to prevent any external penetration.
  - Another critical need was to send different type of traffic and make sure it passes correctly



TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE


Q & A

Get Your Complimentary Amazon Gift Card

Schedule a discovery meeting with one of our industry experts to find the right solution for you and receive a complimentary $50 Amazon gift card.

**First 5 attendees to schedule a discovery meeting will receive a gift card*

How to schedule a discovery meeting?

Contact Brian Tolly
btolly@tempesttelecom.com

TEMPEST TELECOM SOLUTIONS

KEYSIGHT TECHNOLOGIES

AMPERE

Contact Information

Patrick C Miller:
pmiller@amperesec.com | www.amperesec.com | +1.503.272.1414

Eric Floyd:
eric.floyd@keysight.com | www.keysight.com | +1.408.807.8200

Brian Tolly:
btolly@tempesttelecom.com | www.tempesttelecom.com | +1.732.762.3631

TEMPEST TELECOM SOLUTIONS KEYSIGHT TECHNOLOGIES AMPERE