

Detecting and Escalating Cyber Signals in ITS OT Environments

Practical Tips from both the Treat Actor and IT/OT Defender Mindset

Agenda

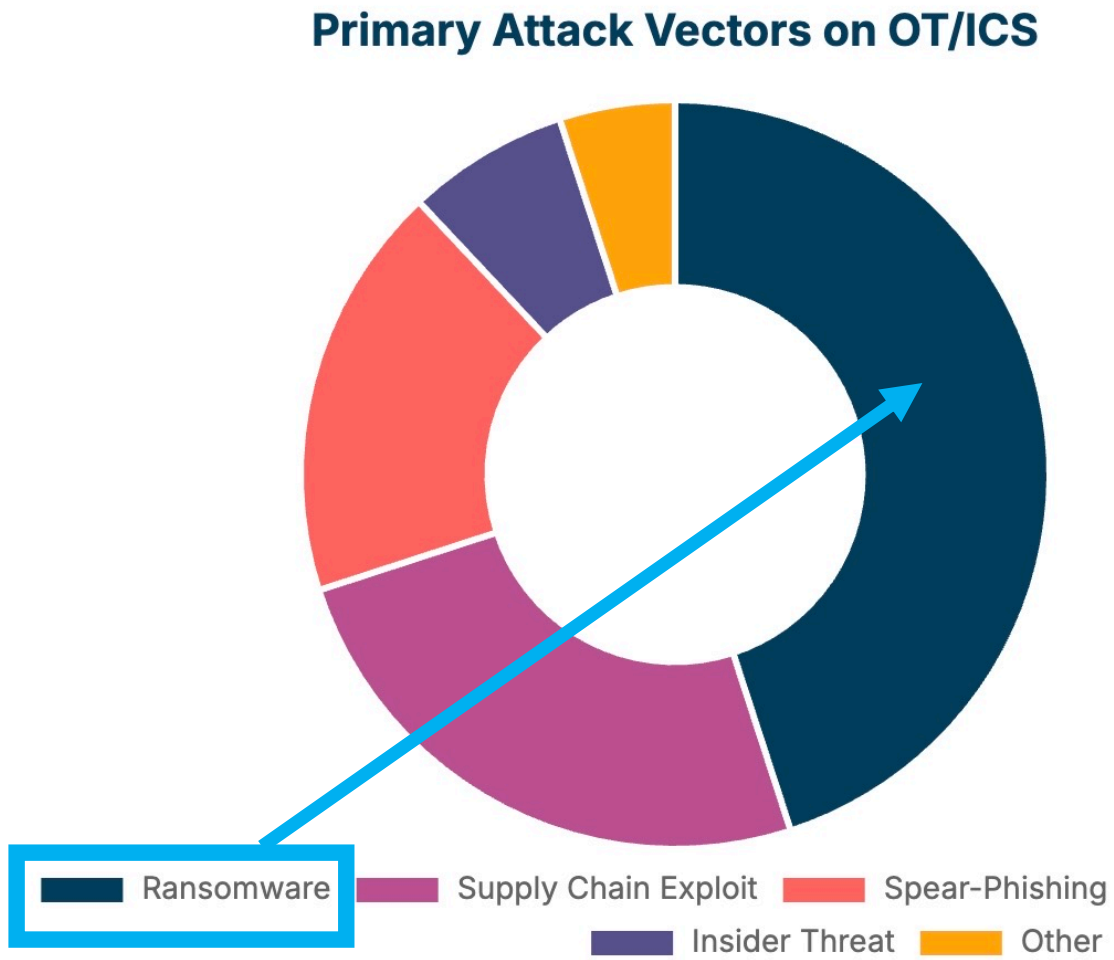
- Key Events and Trends (last 6 months)
- Red Team / Penetration Process with Tales from the Trenches from Years of Attacking and Defending OT
  - Common ICS Environment Entry Points at the Internet/Cloud/Enterprise LAN/WAN
  - Common ICS Environment Entry Points at the IT/OT Boundary
  - Common Firewall and Switch Configuration Errors
  - Attack Vectors for OT and Establishing Persistence
- Why Governance is Important Upfront When Creating Your OT Cybersecurity Program
  - Four Case Studies
  - Roles and Responsibilities
  - RACI Matrix (with input from all roles)
- Assessment should include OT Technical Risks and Physical Security in addition to Policy/Controls Assessment
- Tooling Decisions for Technical Controls Should be Driven by Need
- Creating a Master Risk Register to map real OT risks and remediation strategies to missing technology or process/people projects
- Don't forget about Policies, Procedures, and People (Including educating and uplifting the workforce)
- 3yr Strategic Investment Roadmap for OT Cybersecurity Must Provide Clarity to Executive Board for Finances Required to fund OT Security Initiatives

OT/ICS Cybersecurity Update

> Key Events and Trends (September 2025 – March 2026)

Quick Pulse on Threat Activity

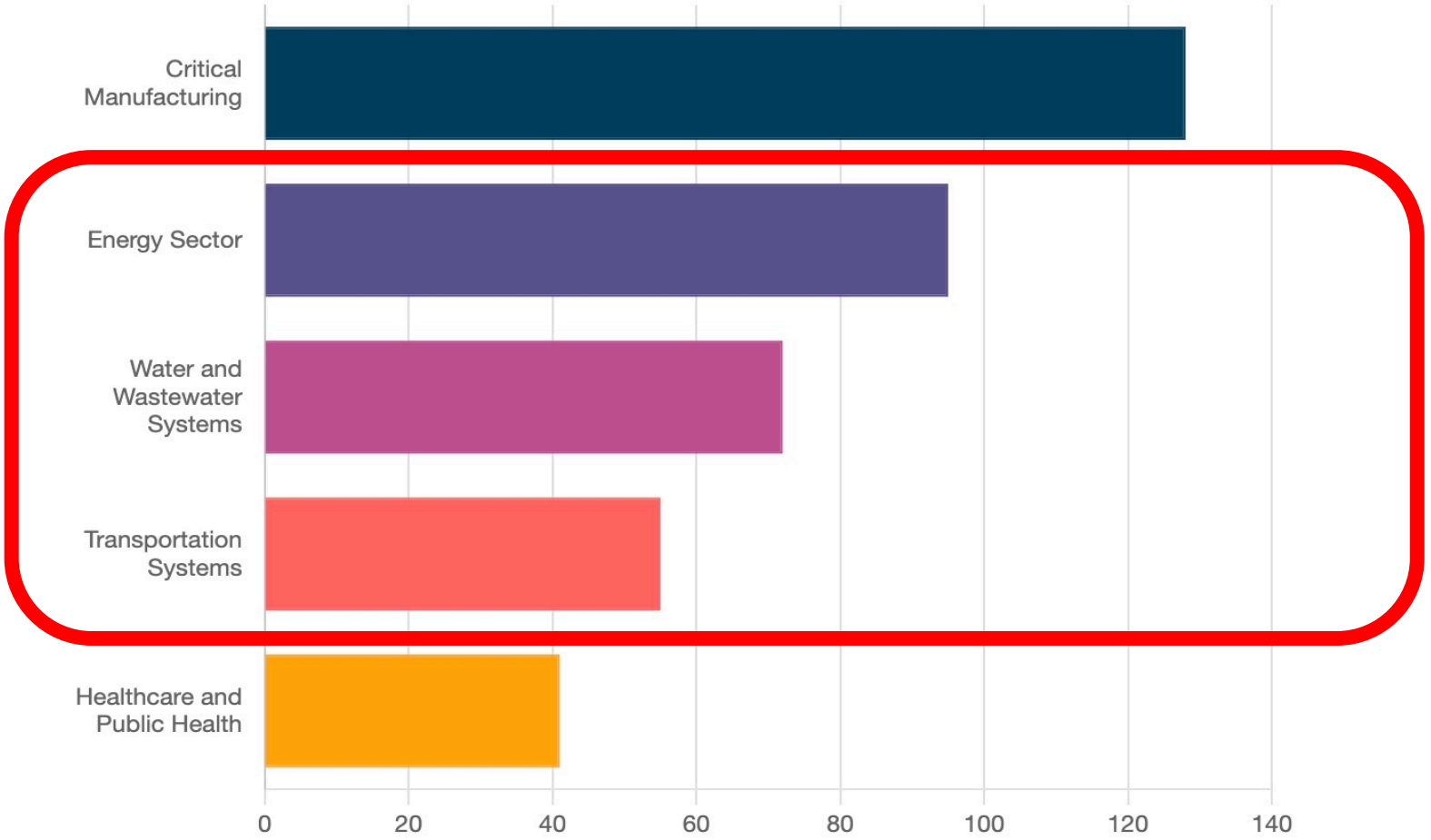
- **78% Year-over-Year increase** in reported cyber incidents targeting national critical infrastructure



OT/ICS Cybersecurity Update

> Key Events and Trends (September 2025 – March 2026)

Reported Incidents by Sector



OT/ICS Cybersecurity Update

> Key Events and Trends (September 2025 – March 2026)

The “Volt Typhon” Kill Chain

- Average Cost of

  $9.4M

  in critical infrastructure sectors > up 15% from 2024

- Average Downtime

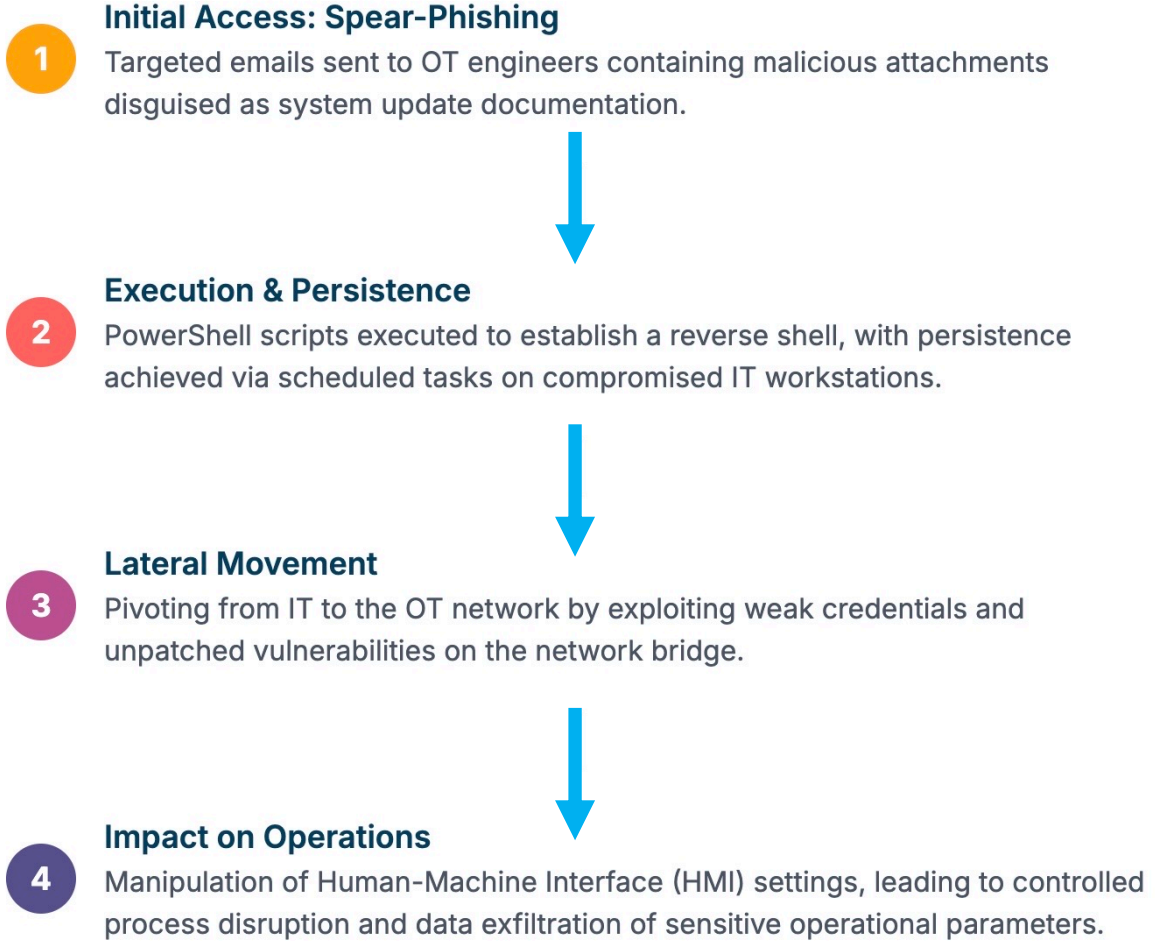
  42 hours

  per incident causing significant production and supply chain loses and delays

- Detection to Containment

  212 days

  the average time to identify and contain a breach in an OT environment

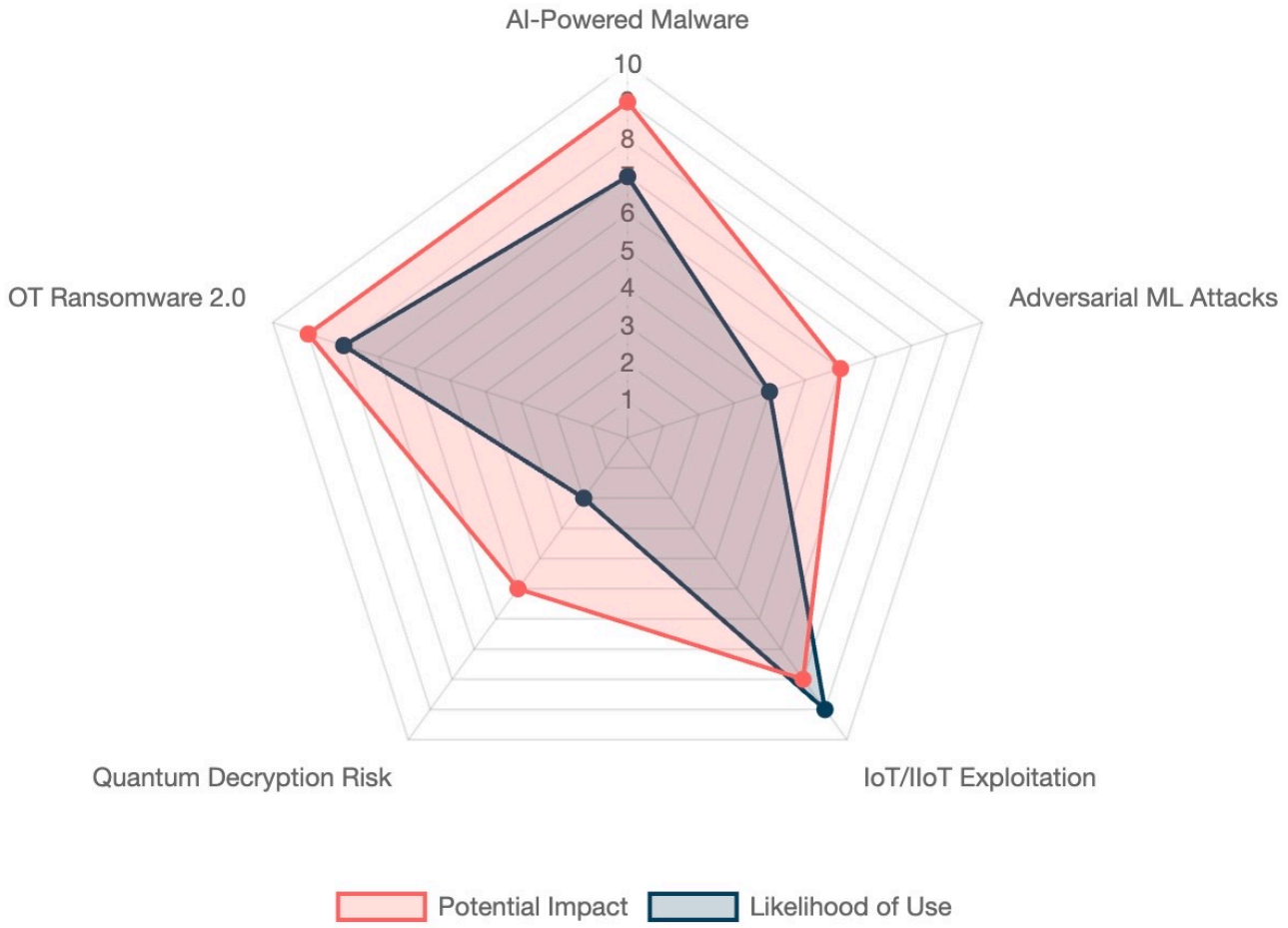


OT/ICS Cybersecurity Update

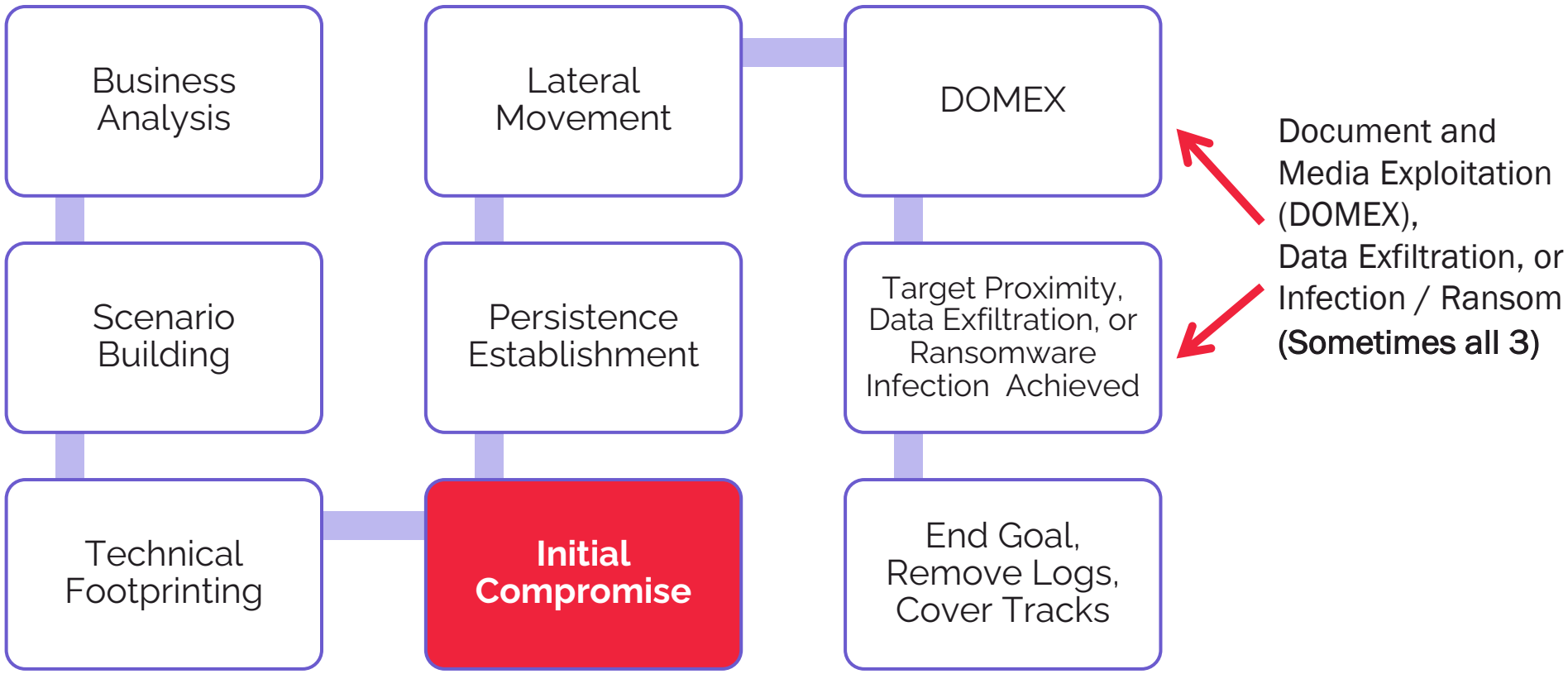
> Key Events and Trends (September 2025 – March 2026)

Projected Risk Landscape

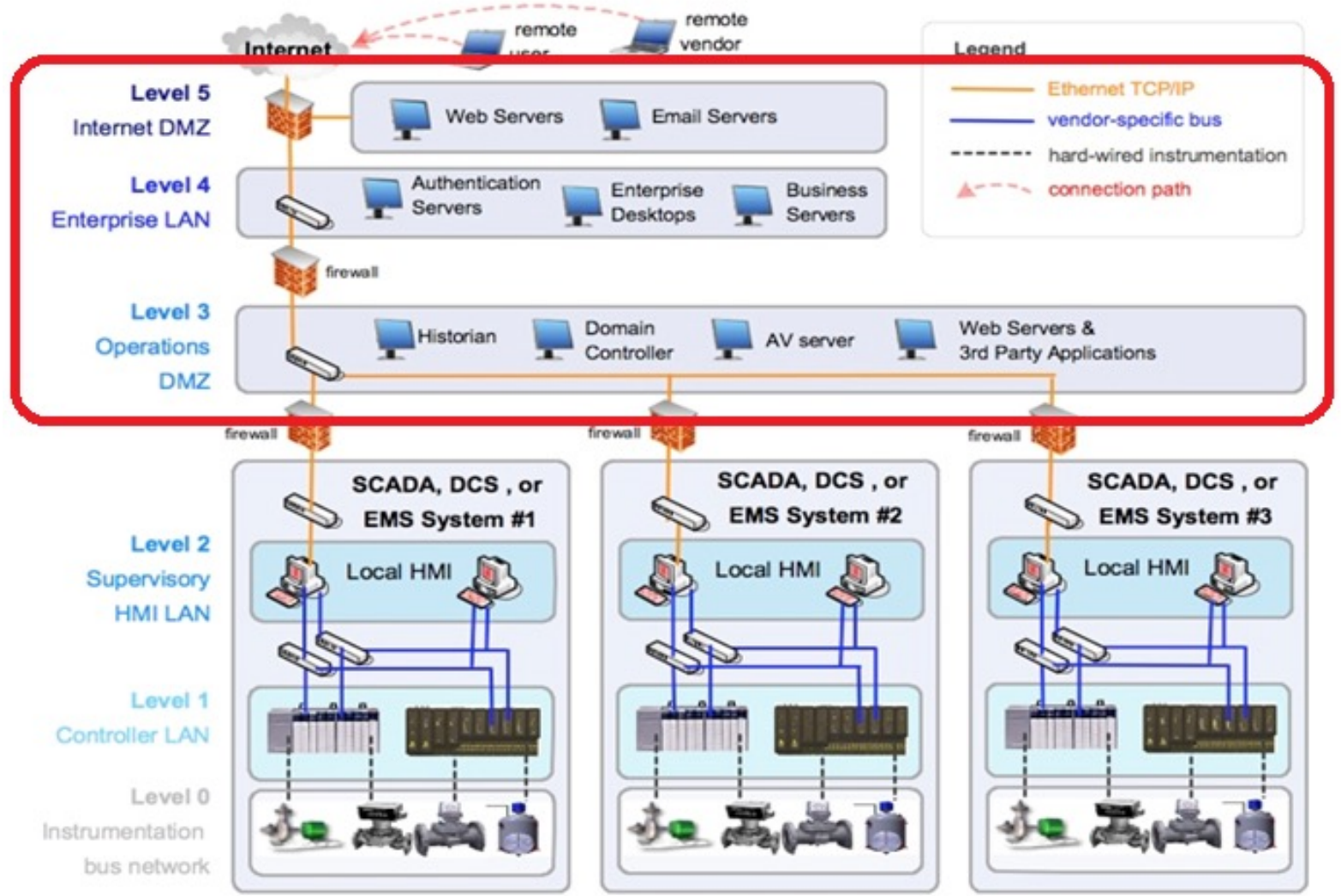
- This radar chart was created by scorin emerging threats on their potential business impact and the likelihood of widespread use by adversaries in the next 12-18 months.
- **AI-powered malware and attacks on converged IT/OT systems** represent the most severe future risks.



Red Team / Penetration Methodology



Common ICS Environment Entry Points at the Internet/Cloud/Enterprise LAN/WAN



ICS Initial Entry Vectors

- Entry Vector **Provides Initial Foot-Hold**
- Can Be Leveraged For:
  - System Pivoting into ‘deeper’ Zones
  - Harvesting Credentials
  - Gathering ICS Environment Intelligence
    - ICS Designs / Documentation
    - Saved System Configurations
    - System Passwords

Level 5 – Internet Based Attacks

- Still a Common Entry Point
  - Access to ICS LAN from Internet Achievable
  - Multi-Zone System Pivoting Probably Required
- Typical L5 Attack Surface
  - Web Applications
  - SSH/FTP/SFTP Servers
  - Email
  - Remote Access
  - Possibly Control Systems Data (Listeners)

Level 5 – Internet Based Attacks

Web Applications

- Corporate Websites
- Board of Directors Portals
- Collaborative Platforms (ex. SharePoint)
  - Communicating with regulators (ex. FERC / MERC / EROs)
  - ICCP transfers between Power Generators / T&D Control Centers
  - Flare Reporting APIs to EPA from Oil & Gas Operators
- Customer Billing Systems
  - Electric Utility Bill Review / Payment
    - Although Frequently Outsourced
  - Energy Market Related Web Services

Level 5 – Internet Based Attacks

Remote Access

- Corporate Cloud VPN & Dial-Up Solutions
- Typically to Corp/Enterprise Network
  - Remote access to remote ICS Systems
    - Distribution & Transmission Substations
    - LNG Pump Station Systems
    - Control Center (ex. EMS) Access
      - Backup/Disaster Recovery Control Centers
        - Also used for data replication
  - Remote Access for Vendor Support
    - Ex. GE “Atlanta Data Highway” (ADH)
    - Turbine / Induction Motor Monitoring (B-Directional Cloud Access for Preventative Maintenance)

Level 4 – Enterprise LAN/WAN Attacks

- Client-Side Vulnerabilities
  - Lots of attack surface
    - Web Browsers
    - Browser Plugins (Flash/Java/Pdf/Silverlight etc.)
    - Email Clients
    - Chat Clients

- Word document / macro's / Adobe framework Vulnerabilities still very effective
  - Especially against EDR's
  - Utilizing PowerShell payloads
  - Living-off-the-land techniques

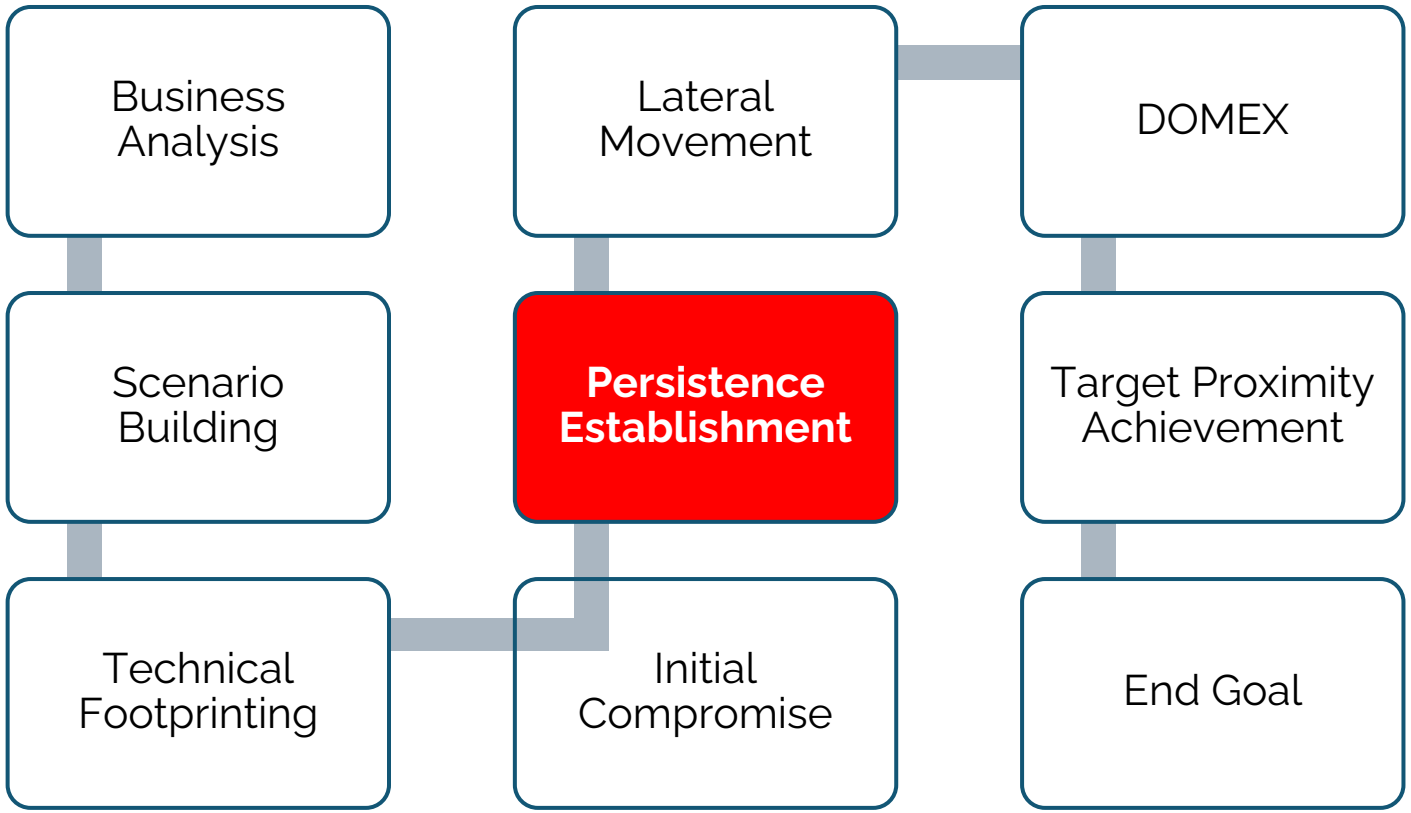
- Building a compelling "phish"
  - Utilize business research to build credibility
  - Offer of a gift card to favorite restaurant / coffee shop
  - Winning technology
  - Expired membership to ICS specific organizations
  - Required corporate or industry training

Level 4 – Enterprise LAN/WAN Attacks

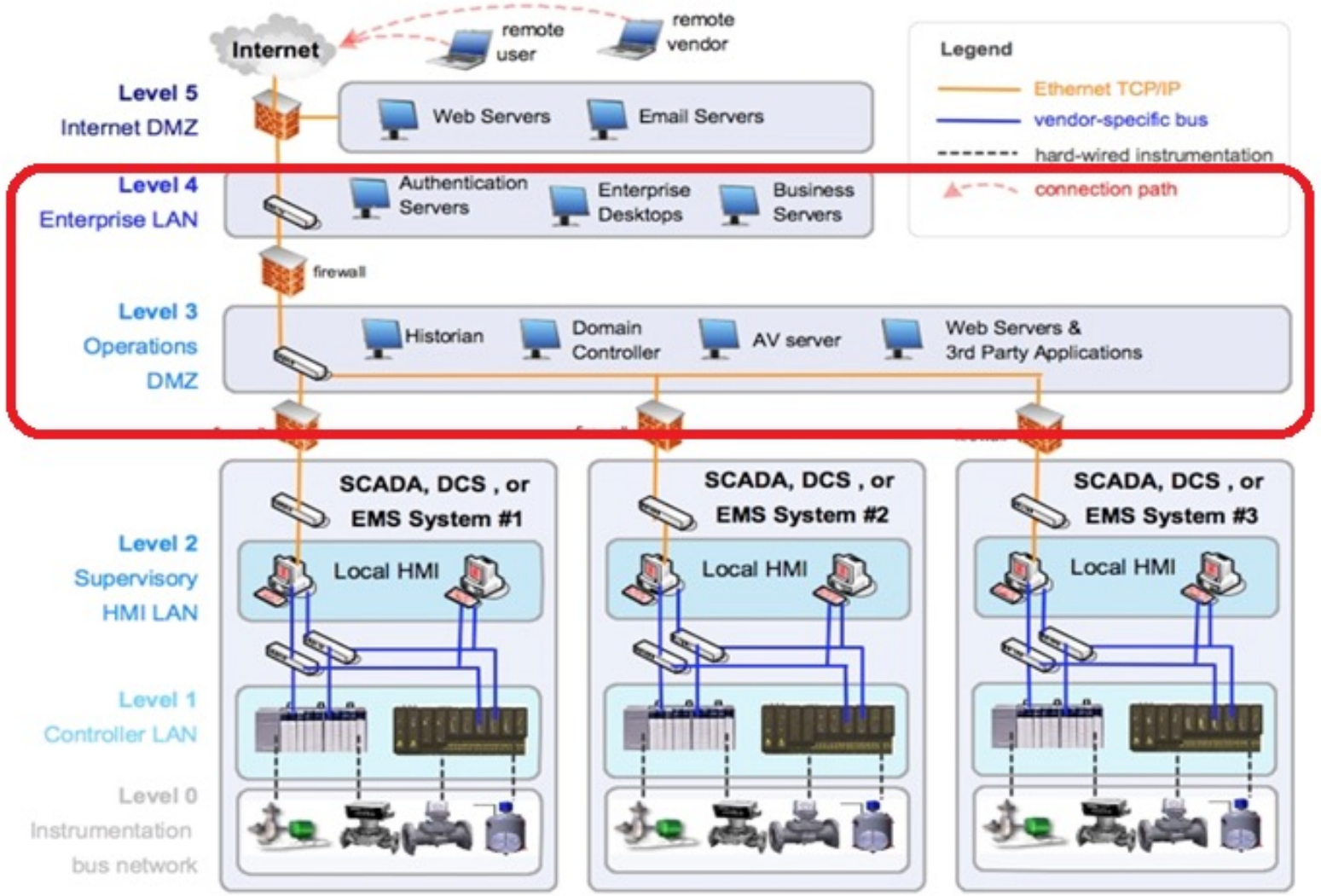
Common Firewall and Switch Configuration Errors

- ICMP and NPT allowed across trust domains provides covert tunneling
- SNMP v1 and 2 disclose community strings in clear
  - Only SNMP v3 encrypts Community strings
  - SNMP v 3 must be “Enforced” because backward compatibility sends the unencrypted strings behind the encrypted ones
  - SNMP community strings allowed to be used to log in administratively
  - SolarWinds compromise was performed long before it was publicized
- Any-to-Any, Any-to-IP ranges, Any-to-TCP/UDP ports and other commonly found unhardened rules
- Use of VLAN ACL (access control lists) instead of Layer 2 physical firewall protection for segmentation
- Firewall / Switch ACL rules often allow ANY networks to access printers and other common office equipment from multiple diverse trust domains
- Flat networks often found at Enterprise LAN/WAN layer that spans multiple geographic locations and multiple departments

Red Team / Penetration Methodology



Attack Vectors for OT and Establishing Persistence



Attack Vectors for OT

Corporate (IT) > OT

- Corporate to SCADA border - Very Insecure
- Data Historians, OPC Servers, Engineering Workstations, and other data connectors are often a bridge to OT Environments.
- Firewall rules for Engineering access or Vendors almost typically found with weak ANY-to-ANY rules allowing anyone from a particular range of IP addresses access to any host or device on the OT side through ANY TCP or UDP port.
- Active X components and outdated Microsoft.Net framework used in the development of many ICS and Web HMI systems – These are highly insecure and vulnerable to exploits available today.
- ICS Systems often contain home-grown applications that do not use secure coding practices. Consider debugging or fuzzing ICS applications to look for undocumented crashes and coding errors.
- Default accounts and passwords are still a HUGE problem - just knowing the vendor of the system is often all the adversary needs to know to access the system and take over control as System Admin.

Attack Vectors for OT

Intrusion Detection Often Not Implemented Properly

- NIDS (Network Intrusion Detection Sensors) often deployed directly on the same logical network as Enterprise LAN / WAN environments and accessible by general user accounts
- NIDS devices have an easily detectable footprint
- NIDS devices can be flooded / disabled and often overlooked as “system glitch”
- Very little use of Intrusion Detection and Network Monitoring in lower networks below the Enterprise IT layer (Level 4)
- IT / OT boundary and in below OT networks often not monitored
- Little collaboration between IT SOC, Outsourced SOC, and OT Engineers
- Little collaboration between Physical Security Surveillance and IT SOC, Outsources SOC, and OT Engineers

Attack Vectors for OT
Remote Access

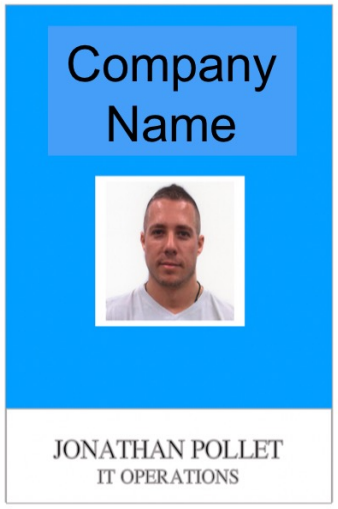
- Dial-up Lines, Modems, etc..
  - Dial-up access still a very viable access
  - no IDS and often no passwords
  - When used, passwords are often a limited number of numerical only digits (like PIN codes) and easy to guess
- Cellular 4G/LTE/5G cards inserted into RTU/PLC Backplanes
  - Usually installed by System Integrators / OEM Support Engineers / Technicians & Contractors
  - Bypasses all protection at higher network layers
  - Provides direct access to all industrial / embedded devices at the control layer (Level 1/0)
- Locally Sourced Internet Connection
  - Internet ISP installed locally at the industrial site by local operations team or contractor to bypass corporate Internet proxy restrictions
- Poorly Configured End Points
  - Engineering Workstations, OPC Servers, PI Servers, Panel PCs, Touchscreen Devices often found with two or more NIC interfaces (Dual or Multi-homed)
  - These systems also often found with Terminal Services (MSclient) / RDP, Radmin, GoToMyPC, TeamViewer or other remote access software installed and left running in “Unattended Mode”

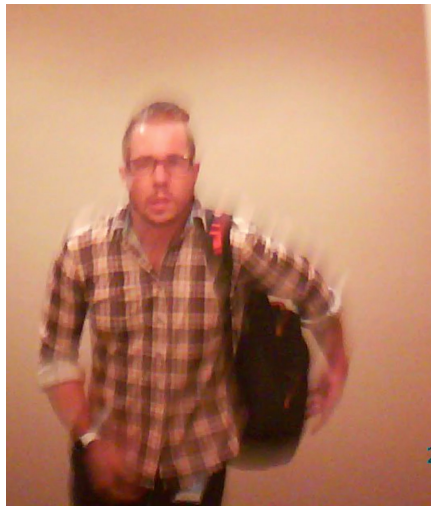
Onsite Physical Access

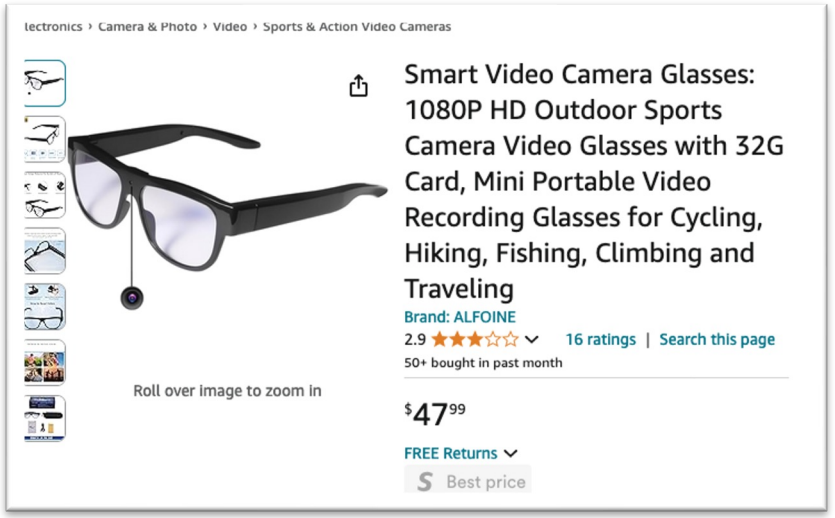
Local RJ45 Ports

- Onsite Physical Access - 100% Success Rate
  - Physical Access to any Corporate PC / network port
  - Open RJ45 ports in publicly available areas make great targets
  - Printers are also excellent places for planting Wi-Fi devices for remote access
  - Walk into any spare office and look like you belong there











Onsite Physical Access

Local RJ45 Ports

- Powered Tap Devices
  - Requires 120V AC or 12V DC
  - Useful if POE tap is required
  - Supports GigE 1000BASET high bandwidth connection points
  - Can tap 2 networks at the same time



Onsite Physical Access

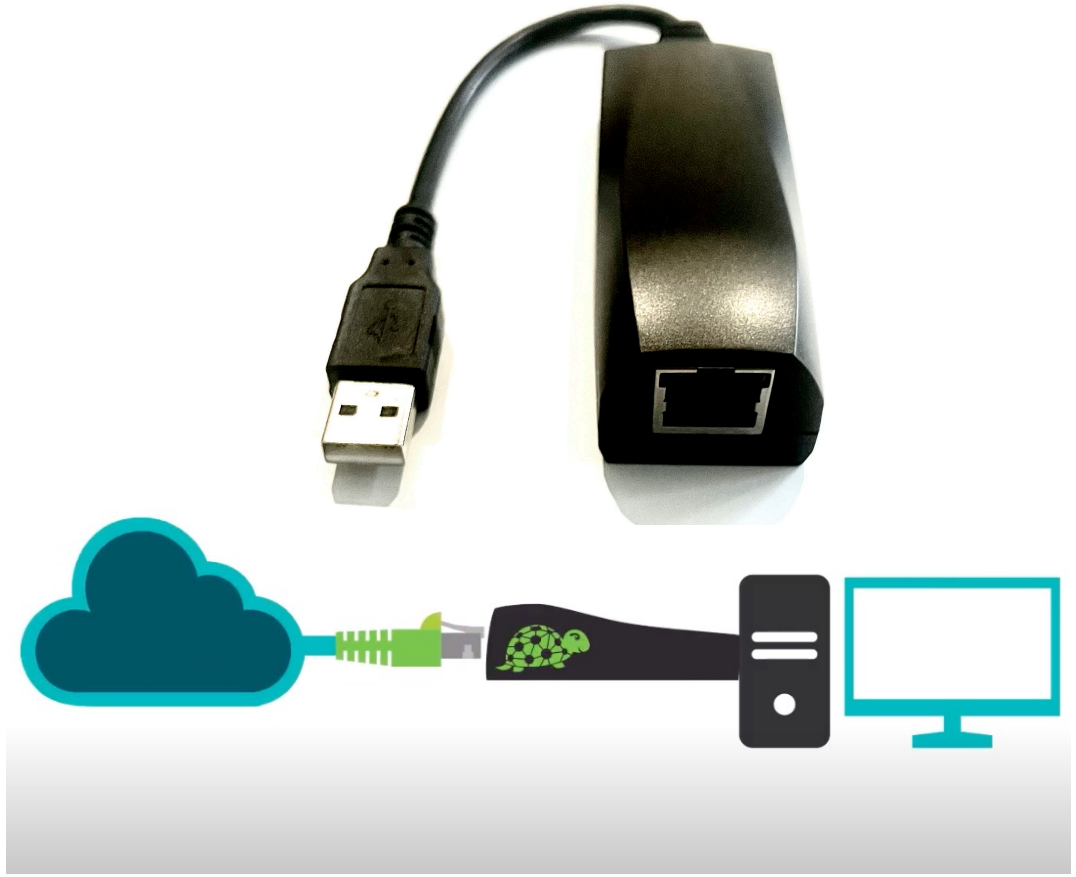
Local RJ45 Ports

- Unpowered Tap Devices
  - Unpowered Passive Ethernet tap
  - Supports 10BASET and 100BASET and forces downgrade of bandwidth on 1000BASET networks
  - Live traffic flows into J1 (left port) and out J2 (right port), then a copy of the data is mirrored on monitoring ports J3 (top port) and J4 (bottom port)
  - **Undetected** when inserted into a network because it is unpowered and has no MAC Addresses > simply maps the internal 8 wires of Ethernet CAT 5/6/7 to additional physical ports



Onsite Physical Access
Local RJ45 Ports

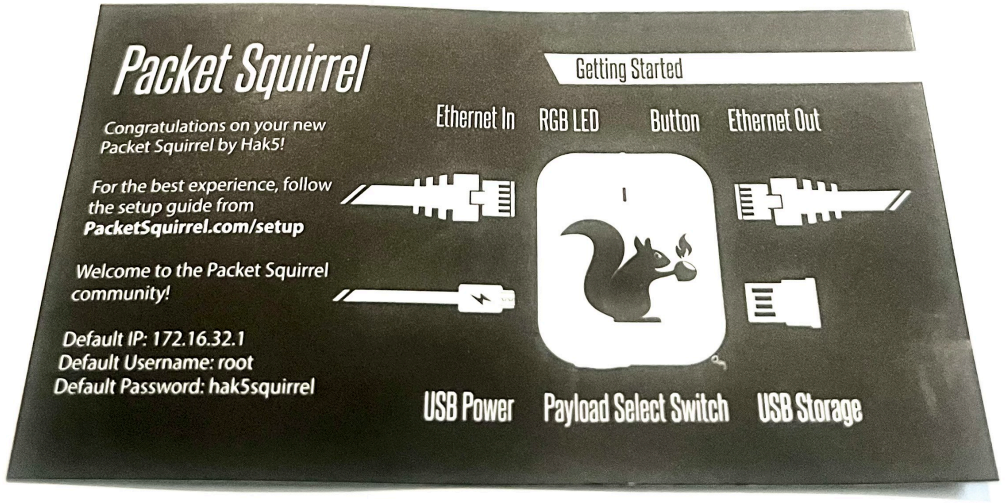
- LAN Turtle
  - Covert Systems Administration and Penetration Testing tool providing stealth remote access, network intelligence gathering, and man-in-the-middle monitoring capabilities
  - Looks like a normal USB Ethernet Adapter



Onsite Physical Access
Local RJ45 Ports

- Pocket Squirrel
  - In-line Ethernet Monitoring and Attack Tool
  - Insert in the line anywhere on a network
  - Can start with it in pass-through mode to start and then flip the switch to activate a full Linux hacking kit with remote access from anywhere in the world
  - Man-in-the-Middle Attacks
  - DNS Spoofing
  - Supports Dynamic Proxy





USB tools

- USB Devices That Require Disk Access (mounting USB)
  - Switchblade (U3 + scripting)
  - Copperfield (H-Worm aka Houdini) RAT
  - SNOWYDRIVE (RAT)
- USB Devices That Masquerade as HID Devices (like a keyboard or mouse)
  - Rubber Ducky
  - BadUSB
  - P4wnP1
- USB Devices That Physically Destroys the Target
  - KillUSB

USB Tools

USB Devices That Require Disk Access (mounting USB)

- Autorun required
- USB3 may also be required
- Often defeated by corporate GPO policy restrictions, registry settings, or antivirus and end-point security software
- A log entry is made each time an external disk is mounted
- Notification or message appears on the user's desktop when a USB stick is mounted
- Stuxnet used this form of attack vector / infection point

USB Tools

USB Devices That Masquerade as HID Devices (like a keyboard or mouse)

- Rubber Ducky USB Kit
  - Autorun not required…
  - U3 not required…
  - Registers as a HID device
  - Requires 30 seconds with a host
  - Can be left behind or retrieved
  - Victim host beacons to a C&C server and can be remotely controlled
  - Accounts, passwords, and any data the host is connected to can be retrieved through Internet connection or stored for later retrieval



USB Tools

USB Devices That Masquerade as HID Devices (like a keyboard or mouse)

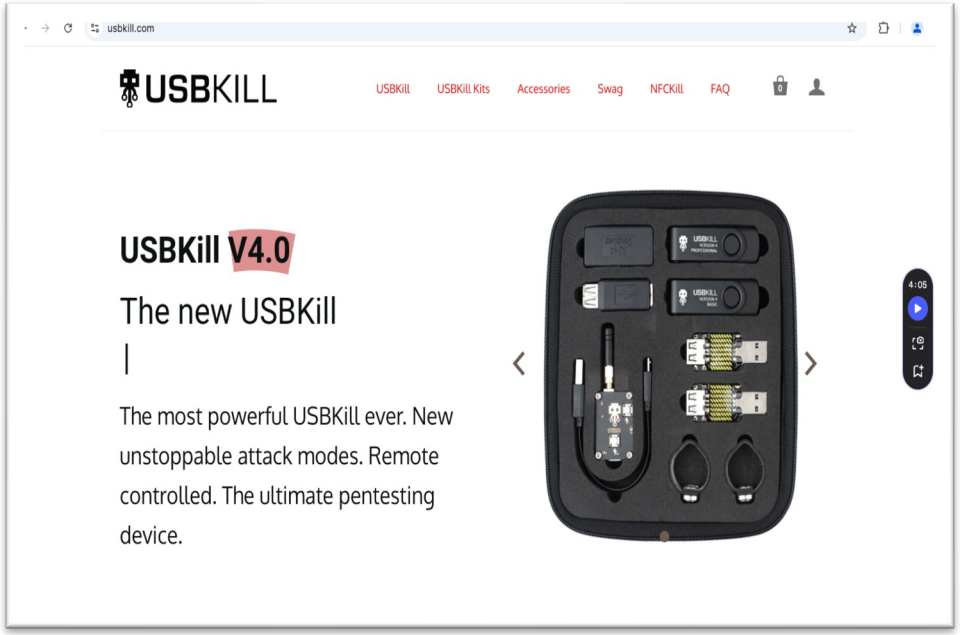
- Anyone Want a Free Mouse?
  - Several gaming devices were carefully taken out of their original packages, the inside areas not needed were hollowed out (machined) and replaced with an Arduino board with multiple on-board USB ports
  - Any payload script could be easily physically inserted into the USB ports and then hidden from the user with a cover that screwed down over the bottom of the mouse
  - The altered gaming devices were sealed again and placed back on shelves at several store locations
  - The altered mouse still registered as the vendor's mouse – as an HID device, however the script waited for 3 minutes of inactivity and then transmitted a string of ASCII codes that launched a command prompt and exported the local SAM file along with other key Windows files to a remote C&C server where rainbow tables were able to quickly crack the local and admin accounts



USB Tools

USB Devices That Physically Destroys the Target

- KillUSB (Physical Destruction)
  - A traditional USB-A port typically delivers 5 volts (5V), with power ranging from 2.5 watts (for USB 2.0) to 4.5 watts (for USB 3.0)
  - The KillUSB Kit uses internal diodes and capacitors to take the normal power delivered out of the USB port, store it, add it back to the input power, and repeat over thousands of times to crank up the voltage and amps and then delivered back into the USB port
  - Within seconds, the computer, TV. Printer, projector, etc. goes black and will not reboot. Device must be thrown away. Often results in physical smoke coming out of the computer, server, or any device that has a USB port
  - Supports over 15 different industry standard local device ports
  - Can be inserted into any port (i.e., USB-A, USB-C, Lightning, VGA, HDMI, MicroUSB, etc.)
  - The device can be triggered with a date/time script or with an RF remote



Asset Owner Profile

> Pipeline / Transportation

Large North American Pipeline Company

- A diversified energy company, uniquely positioned to help accelerate the global energy transition through ethical, sustainable and socially responsible methods.
- Their four core businesses include:
  - Liquids pipelines
  - Natural gas pipelines
  - Gas utilities and storage
  - Renewable energy
- Operational Technologies (OT) and Industrial Control Systems (ICS) are integral to these processes, automating critical operations, detecting and preventing leaks and environmental hazards, while ensuring the safety of the equipment and personnel in the area.

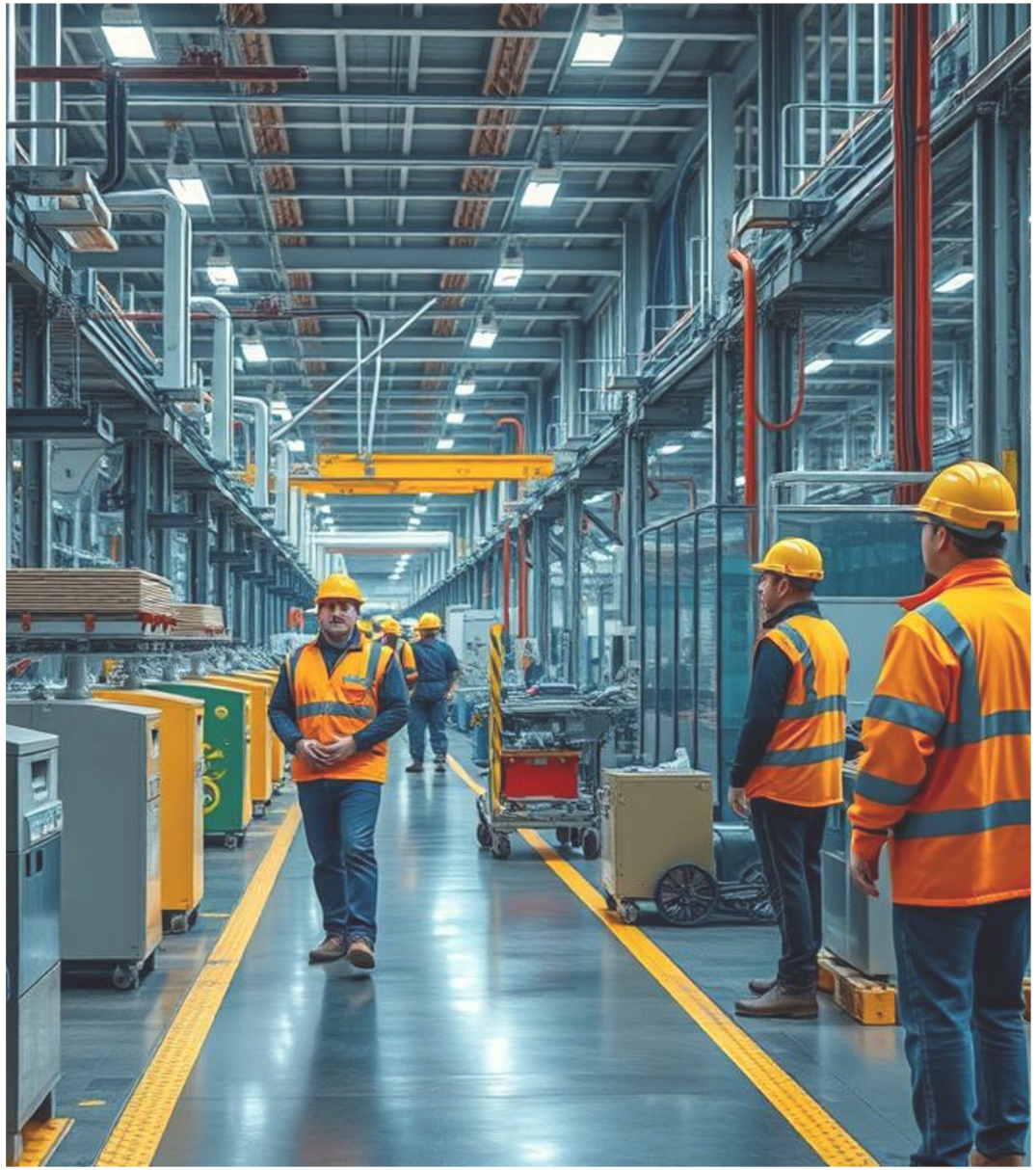


Asset Owner Profile

> Manufacturing

Global Manufacturer

- A global leader in the beauty industry, recognized for its portfolio of iconic brands in color cosmetics, skincare, hair care, and fragrances.
- The company operates in more than 150 countries, serving a diverse customer base with products that transform the lives of consumers.
- Operational Technologies (OT) and Industrial Control Systems (ICS) are integral to the manufacturing processes, automating critical operations and ensuring efficiency.



Asset Owner Profile

> Electric Power Utility

Asian Electric Power Utility

- One of the longest-established power companies in the world. This Electric Power Utility has a world-class record of providing a highly reliable electricity supply to several island communities in Asia.
- Electricity is generated at the Company's power station on one Island which uses natural gas and coal as fuels. Electricity is then transmitted and supplied via an extensive cable network to customers. The generation, transmission and distribution of electricity are monitored and controlled by the System Control Center, which uses advanced technologies to ensure supply reliability round the clock.
- To support the development of renewable energy, the utility has commissioned the region’s first commercial scale wind power station and a 1 MW solar power system inside the main Power Station. The solar power system is one of the largest solar power systems in the region.



Asset Owner Profile

> Airport / Transportation

Middle East Major Airport

- Considered one of the busiest airports in the world, this airport in the middle east welcomes nearly 100 million guests a year, reaffirming its status as the world's leading international airport for over 10 consecutive years.
- Connected to over 250 destinations by more than 100 international carriers, this airport has established itself as a preeminent global hub.
- Over a dozen critical real-time industrial OT systems are required to function without failure around the clock to enable efficient airport operations.



Governance Challenges

Key Governance Issues

- Lack of clear roles and responsibilities can lead to gaps in cybersecurity oversight.
- Current governance structure does not effectively empower OT security leadership
- Realign the Governance Structure to Create and Empower a Centralized OT Security and a Centralized Physical Security Leadership role with existing teams at the industrial level providing local "Champions."
- Insufficient resources allocated for comprehensive cybersecurity remediation efforts.
- More FTEs needed for daily automation, engineering, and cyber security resources to handle large scope of cyber security remediation needed across the organization.

Standardize OT Cyber Security Policies and Processes

- Review existing Cyber Security policies created for the Business IT systems, compare them to regulations and requirements for critical infrastructure and industry best practices, to expand the existing policies to include the OT / Site Operations systems.
- Communicate new OT cyber security policies and processes to all affected operational roles

Training and Awareness Needs

- Cybersecurity training is essential for all employees with security responsibilities.
- Regular updates and awareness campaigns can improve compliance and vigilance.
- Establishing a culture of security is vital for proactive risk management.



Roles and Responsibilities

- Establish centralized governance roles specifically for OT security, ensuring accountability and clear lines of authority.
- Create an OT Cyber Security Committee to oversee and coordinate security efforts across all manufacturing facilities, enhancing collaboration between IT and OT teams.
- Develop and expand existing security policies to encompass OT environments, aligning them with industry best practices and regulatory requirements.
- Implement a continuous training program for all personnel involved in OT security, focusing on emerging threats and best practices for risk management.
- Evaluate and adjust security strategies regularly to adapt to new technologies and evolving cyber threats, ensuring the organization remains resilient.

RACI for all Roles that have Security Assurance Responsibilities

OT Security Policy Areas	IT Operations Admin Team	Security Operations Center (SOC)	OT Monitoring and Incident Response	Business Continuity Management	Information Security Governance Team	OT Security Lead	OT Security Engineer(s) (coordinates security requirements with OT sites)	Cybersecurity Point of Contact at the OT site (Designated point of contact at each OT Site for Cybersecurity responsibilities)	OT Engineering Team	Local OT Maintenance Team	OEM Vendor
Groups / Roles and their Responsibilities for Maintaining Security of OT Systems											
Business Environment and Understanding the Role in Critical Infrastructure Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Governance Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Risk Assessment Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Risk Management Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Awareness and Training Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Secure Architecture Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Follow Policy
Data Protection Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Sets Policy and Communicates to all	Responsible to Implement	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Provides Input for Solutions that Work with OT Systems
Capacity Planning and Prioritization Policy	Reports OT Capacity Constraints and Risk up to IT Security and	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Reports OT Capacity Constraints and Risk up to IT Security and	Responsible to Implement	Assists in Communicating Policy with OT Sites	Assists in Communicating Policy with OT Sites	Tracks and Reports Capacity Needs	Tracks and Reports Capacity Needs	Assists OT Maintenance Team
Data Leakage Policy	Assists in Policy Development	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Sets Policy and Communicates to all	Responsible to Implement	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Provides Input for Solutions that Work with OT Systems
Software/Hardware Integrity Assessment Policy	Informed	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Provides Input for Solutions that Work with OT Systems
Development and Testing Environment Policy	Informed	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Responsible to Implement	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Assists in Communicating Policy with OT Sites and Implementing Required Solutions	Follows Policy and Informs OEM Vendors	Follows Policy and Informs OEM Vendors	Provides Input for Solutions that Work with OT Systems
Baseline Configuration Policy	Informed	Informed	Informed	Sets Policy and Communicates to all	Assists in Policy Development	Consulted	Informed	Informed	Responsible	Follows the policy	Provides Input for Solutions that Work with OT Systems
System Development Lifecycle Policy	Informed	Follows Policy and Informs Team Members	Follows Policy and Informs Team Members	Sets Policy and Communicates to all	Assists in Policy Development	Consulted	Informed	Informed	Responsible	Follows the policy	Provides Input for Policy and Supports OT Teams

Types of Responsibility	Color Code
Color Code Legend	
(R) Main Responsible Party or Responsible to Implement	(R)
(A) Accountable	(A)
(C) Consulted	(C)
(I) Informed	(I)

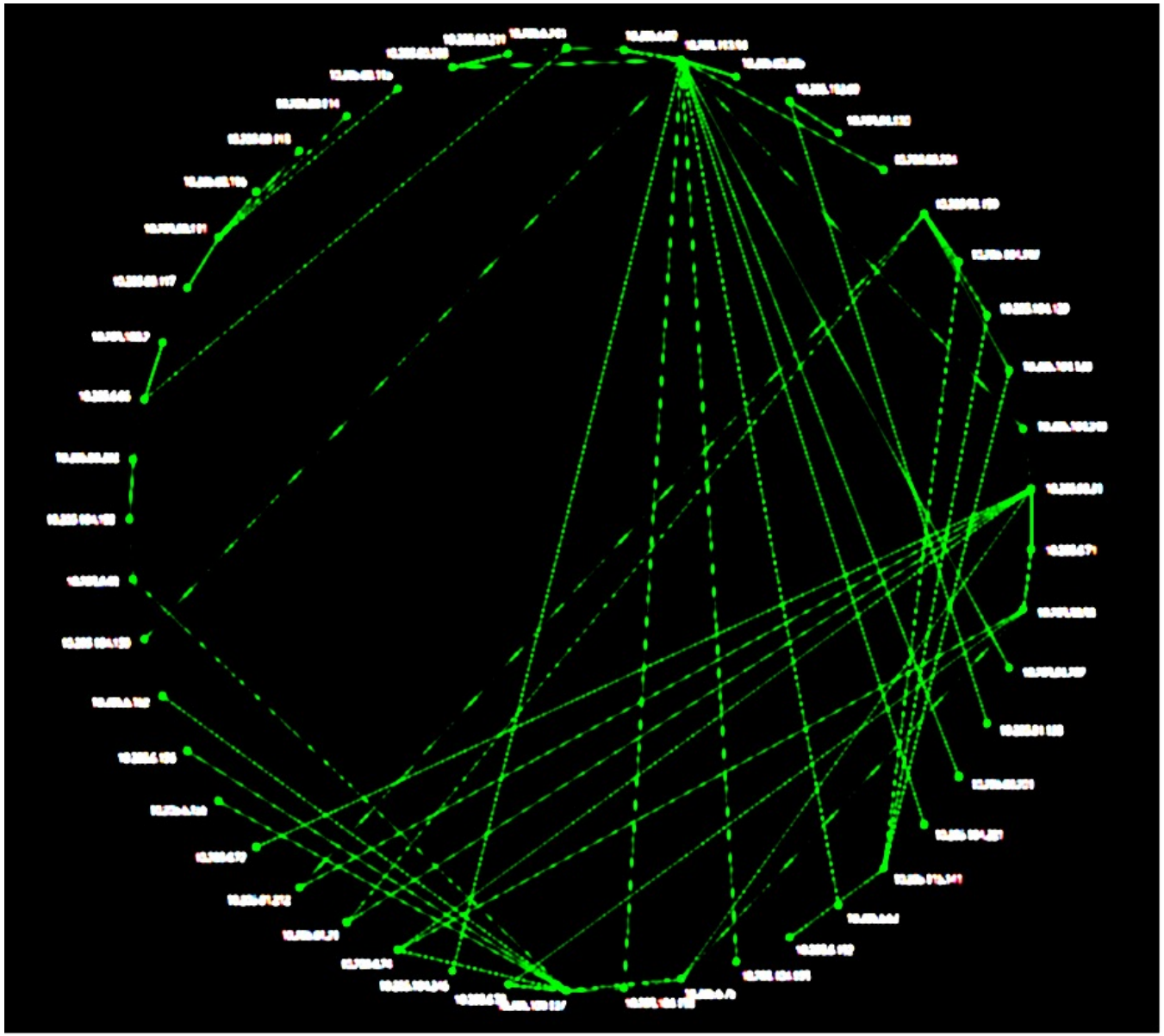


Top Trending OT Technical Risks

1. **Enhance Network Segmentation:** Aggressively enforce micro-segmentation between IT and OT networks. Verify and audit firewall rules to prevent unauthorized lateral movement.
2. Implement a centrally managed but locally deployed Ransomware-proof **Resilient Backup and Restoration solution**
3. Prioritize Asset Visibility: Invest in solutions for **comprehensive OT asset inventory and vulnerability management**. You cannot protect what you cannot see.
4. Develop a **Converged SOC:** Integrate OT monitoring and incident response into your Security Operations Center (SOC) to provide a single pane of glass for threat detection and response.
5. **Conduct Regular OT-Specific Drills**: Run tabletop exercises and red team/blue team drills that simulate attacks on your specific industrial control systems and processes.

Explore IT/OT Network Interdependencies

> capture and analyze live traffic (PCAP)



Tooling Decisions for Technical Controls Driven by Need

Asset Management Issues

Asset management for industrial control systems is primarily ad hoc, relying on outdated spreadsheets. **Real-time monitoring tools are available from Fortinet, Palo Alto, Nozomi Networks. Dragos, and other providers that can enhance visibility and alert capabilities.**

Remote Access Control Risks

Remote access protocols like RDP and TeamViewer are overly permissive, allowing connections from any device. **Immediate restrictions, a secure jump server setup, with enforced MFA are necessary.**

Legacy System Vulnerabilities

Many OT systems operate on outdated, unsupported operating systems, increasing susceptibility to malware. Outdated commercial off-the-shelf network hubs to be replaced with industrial switches made for industrial environments. **Upgrades to modern systems should be prioritized to mitigate these risks.**

Network Architecture Weaknesses

The existing network architecture separates IT and OT environments using VLANs, however **information can pass directly between IT and OT networks without passing through a middle neutral DMZ network.** The current architecture lacks segmentation. This increases risk as malware can traverse between networks without proper isolation. Firewalls with deep packet inspection or dedicated data-diode devices may be required for high-risk connections.

Patching, End Point Protection, Backups, etc.

Technology, processes, and FTE staff required to implement a more robust and repeatable vulnerability and patch management system is needed whereby the windows-based computers supporting the OT processes can be easily updated and patched on a periodic repeatable period at least once a quarter. **End point protection centrally managed through the new DMZ can** provide a consistent approach for securing legacy dated systems that can’t be patched. **A centralized ransomware-proof backup solution is needed.**

Physical Security Findings

Current Physical Security Measures

- Most industrial facilities employ multiple layers of physical security including fencing, gates, and security personnel.
- Access control is managed through a combination of physical locks and badge access systems.
- Proximity RFID badge cards are used for controlled access, but many areas still rely on traditional keys.

Recommendations for Improvement

- **Expand the use of MAG locks and digital access badges to replace traditional lock-and-key system wherever possible**
- Implement logging for access control to track entry and exit times more effectively.
- **Enhance surveillance coverage where industrial cabinets containing OT/ICS components or IT racks housing networking equipment can be accessed**
- Introduce additional layers of security, such as biometric access controls, for sensitive areas.
- **Integrate physical security alerts with SIEM for correlation**



Create a Master Risk Register

Major Risks Identified

The assessment uncovered several high, medium, and low severity risks linked to cybersecurity vulnerabilities in OT/ICS environments.

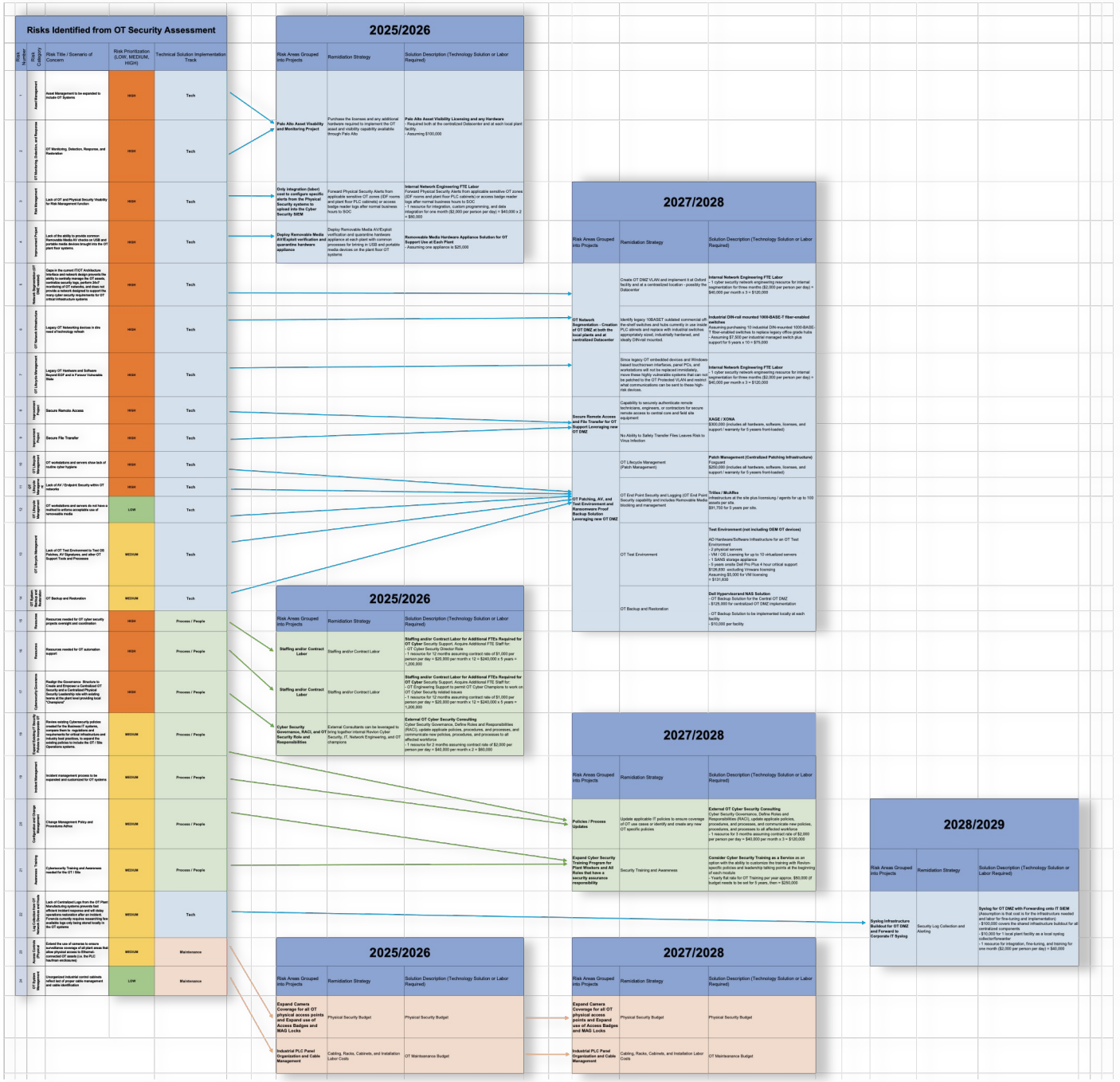
High Severity Risks

Critical vulnerabilities include outdated operating systems, inadequate remote access controls, and lack of network segmentation, which expose the facility to malware and ransomware.

Remediation Priorities

Immediate focus on patching legacy systems, enhancing physical and cyber security controls, and implementing robust governance to address identified risks.

Group Risk Remediation into Technology, Process/People, and Maintenance Projects for a 3 Year Strategic Roadmap



Summary and Q&A

Jonathan Pollet, CISSP, CAP, PCIP
Founder and Sr. Security Consultant
Red Tiger Security
office: +1.877.387.7733
mobile: +1.281.748.6401
jpollet@redtigersecurity.com