NAVIGATING THE ICS AND OT THREAT LANDSCAPE: LEVERAGING RISK ASSESSMENTS TO MITIGATE FEAR

FOCUS ON THE WHAT AND THE WHY, THEN FIGURE OUT THE HOW!

- ONLY 52% OF ICS/OT FACILITIES HAVE AN ICS SPECIFIC INCIDENT RESPONSE PLAN
- 38% OF COMPROMISES TO THE ICS SYSTEM COMES IN THROUGH THE IT NETWORKS
- 47% OF PENTESTING IS AGAINST LEVEL 2 ON THE PURDUE MODEL
- 22% OF FACILITIES ARE USING THE MITRE ATT&CK ICS TO UNDERSTAND MODERN ICS THREAT DETECTION
- DEPLOYING TRAINED DEFENDERS TO LEVERAGE ICS SPECIFIC NETWORK VISIBILITY

FOCUS ON WHAT & WHY

IDENTIFY CRITICAL ASSETS AND SYSTEMS:

Determine which assets and systems are critical to the operation of the ICS environment. This includes identifying all physical and logical components, such as SCADA systems, PLCs, RTUs, HMI devices, and network infrastructure.

DEFINE AND UNDERSTAND THE SCOPE:

Clearly outline the scope of the assessment. This includes specifying the boundaries of the ICS environment, the systems to be included, and the depth of the assessment.

CONDUCT A THOROUGH INVENTORY:

Create an inventory of all ICS components and their configurations. This should include hardware, software, firmware versions, network connections, and communication protocols.

IDENTIFY THREATS AND VULNERABILITIES:

Identify potential threats that could exploit vulnerabilities in the ICS environment. Consider both external threats (e.g., cyber-attacks, malware) and internal threats (e.g., insider threats, system misconfigurations).

ASSESS SECURITY CONTROLS:

Evaluate existing security controls in place to protect the ICS environment. This includes physical security measures, network security controls, access controls, and policies and procedures.

ANALYZE RISK:

Conduct a risk analysis to determine the potential impact and likelihood of identified threats exploiting vulnerabilities. Use a risk matrix or similar tool to prioritize risks based on their severity and probability.

DOCUMENT FINDINGS AND RECOMMENDATIONS:

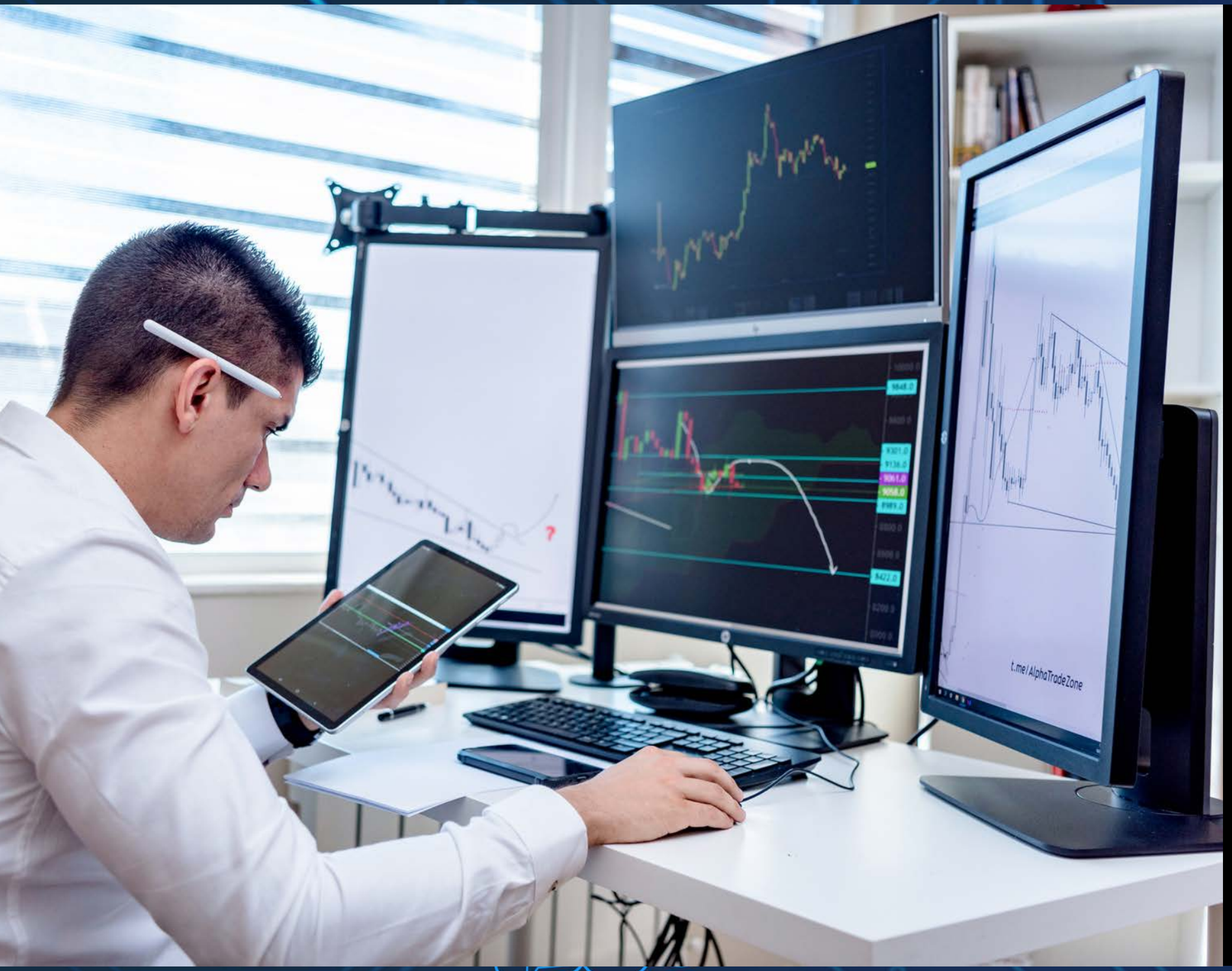
Document the findings of the assessment, including identified gaps and vulnerabilities. Provide actionable recommendations for mitigating risks and enhancing the security posture of the ICS environment.

DEVELOP A MITIGATION PLAN:

Develop a detailed plan to address the identified risks and gaps. This plan should prioritize actions based on the risk analysis and include timelines, resource requirements, and responsible parties.

IMPLEMENT SECURITY ENHANCEMENTS:

Execute the mitigation plan by implementing recommended security enhancements. This may involve updating software, patching vulnerabilities, enhancing access controls, and improving network segmentation.



MONITOR AND REVIEW:

Continuously monitor the ICS environment for new threats and vulnerabilities. Regularly review and update the risk assessment and mitigation plan to adapt to changing security landscapes and emerging threats.

CONDUCT REGULAR TRAINING AND AWARENESS:

Provide ongoing training and awareness programs for staff involved in the ICS environment. This ensures that personnel are knowledgeable about security best practices and emerging threats.

ENGAGE IN CONTINUOUS IMPROVEMENT:

Foster a culture of continuous improvement by regularly reassessing the ICS environment and refining security controls. Incorporate lessons learned from incidents and near-misses to enhance the overall security posture.

ALETA Technologies

AARON BURROWS

(256) 303 - 2889

aaron.burrows@aletatechnologies.com