OT Workshop

Simplify Your OT Security Roadmap

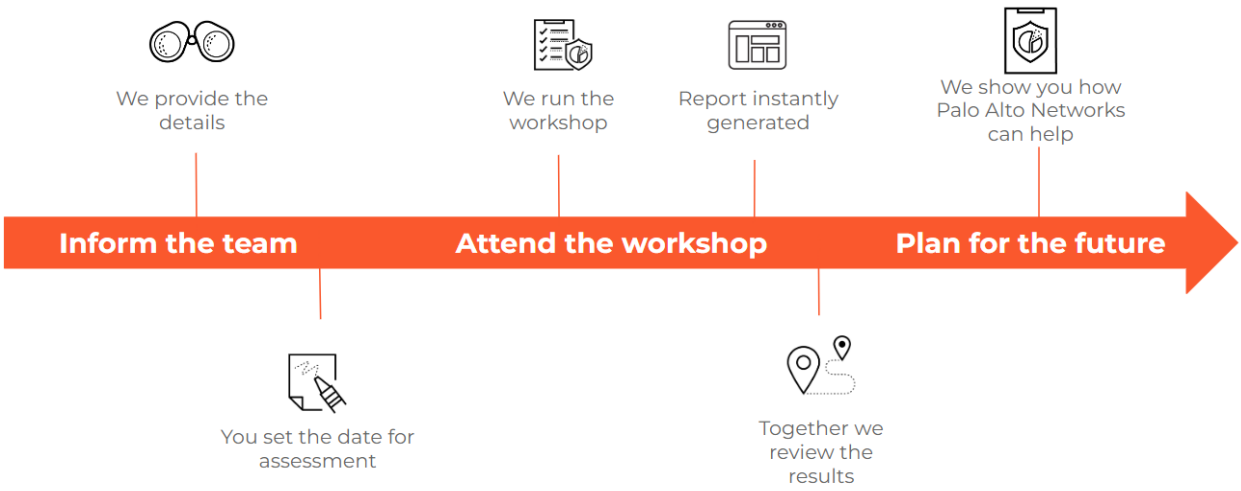
The OT Assessment protects you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

Overview

Reducing cyber risk and costs can't come at the expense of building a business that is equipped to meet new challenges and opportunities. Our OT Assessment can help you reduce risk and improve operational resilience, so you can embrace digital with confidence. We offer a complimentary OT assessment that is tailored to your organisation's cyber maturity objectives. By understanding your current security posture, we design a roadmap that's right for you.

The OT Assessment covers the following technology areas and takes approximately one hour to complete.

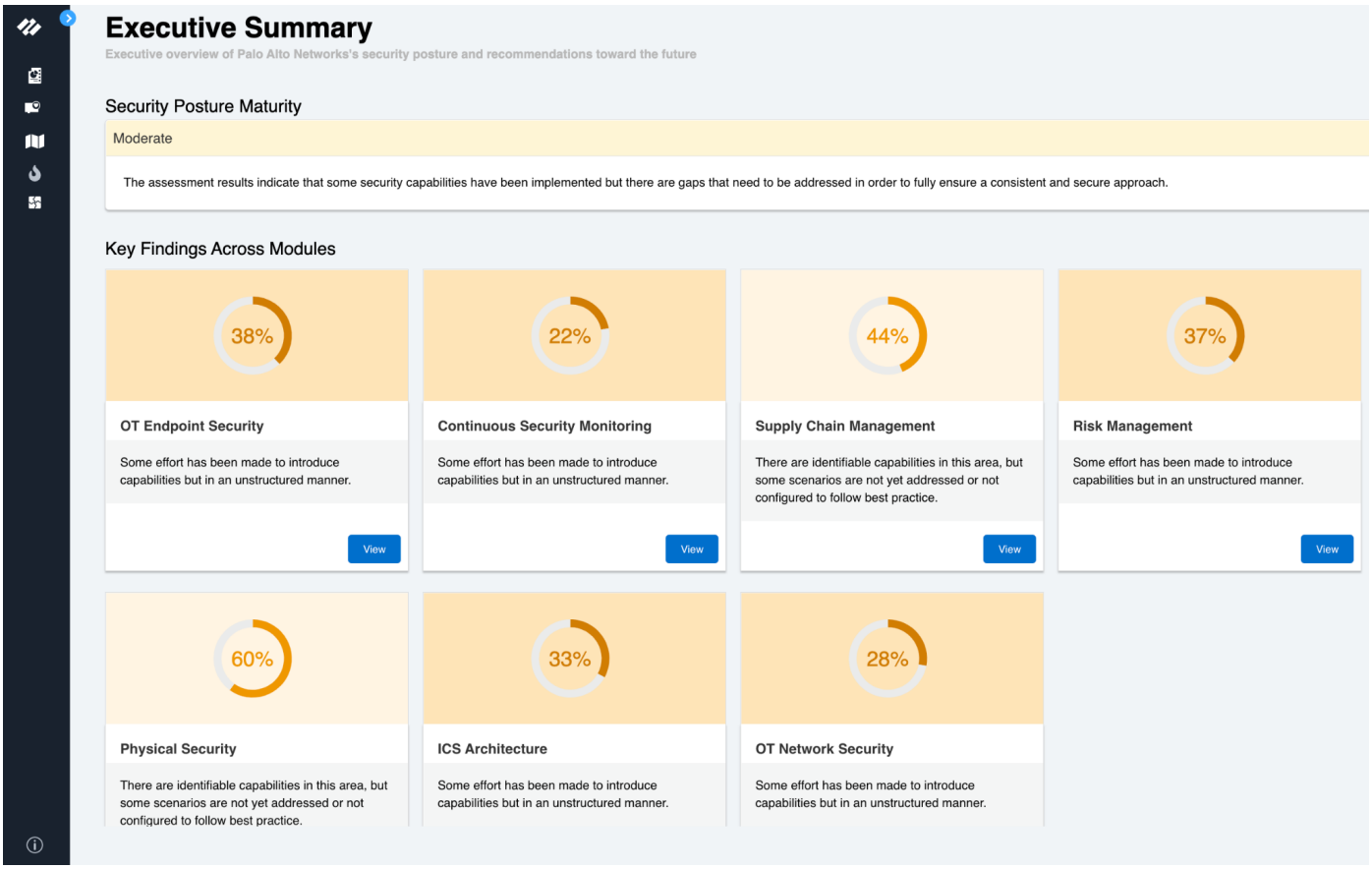
- Risk Management
- Physical Security
- ICS Architecture
- OT Network Security
- OT Endpoint Security
- Continuous Security Monitoring
- Supply Chain Management



What you can Expect

- An accurate analysis of your current security posture with regards to all the components that make up your OT enviro=nment.
- Enablement of security teams so you may best optimize existing technologies
- Reduction in overall business risk by incorporating new technologies and security controls.
- A comprehensive plan for the future as OT and IT networks converge.

Fig 1: Executive Summary - aggregate, non-technical view of significant overall findings.



Who should attend the workshop

The following roles at your organisation should be invited to attend the session:

- OT Security Architects
- Network and Infrastructure Operations
- Data Privacy Officer or Cyber Risk Analyst

The workshop comprises the following Security capabilities and questions:

We assess your organisation's OT Security Capability maturity against in the OT Technology Categories.

Technology Category	Security Capability	Question
Risk Management	Risk and Governance	Do you have a comprehensive catalog of your OT/IOT assets? Is this dynamic or static?
Risk Management	Risk and Governance	Does corporate cyber risk management also extend to cover the Operational Technology environment?
Risk Management	Risk and Governance	Does the organisation have clear ownership and accountability for OT cyber security?
Risk Management	Risk and Governance	Is OT cyber investment based on risk analysis?
Risk Management	Risk and Governance	Do you have an OT incident response capability provided either internally or externally?
Risk Management	Risk and Governance	Does your business continuity plan include OT?
Risk Management	Risk and Governance	Do you have a disaster recovery plan for OT?
Risk Management	Risk and Governance	Do you identify sensitive content including telemetry in network traffic from the ICS?
Risk Management	Risk and Governance	Do you prevent sensitive content including telemetry from leaving the network from the ICS?

Technology Category	Security Capability	Question
Physical Security	Physical Access	Are key OT sites physically secure with the basics such as door locks and CCTV?
Physical Security	Physical Access	Are key staff vetted to a minimum level? e.g. control system staff.
Physical Security	Physical Access	Do you have a 24/7 monitored security systems and physical response?
Physical Security	Physical Access	Are staff educated on security threats, behavior and best practices?
Physical Security	Physical Access	Is Multi-Factor Authentication in place to control access to critical systems and applications?
ICS Architecture	Segmentation and Control	How do you segment within your OT environment to prevent lateral threat movement?
ICS Architecture	Segmentation and Control	Do you segment your legacy technology and smart technology?
ICS Architecture	Segmentation and Control	How do you detect and manage bridging between IT and OT environments?
OT Network Security	Edge and OT Network	Is a network-level Vulnerability protection solution in line for all traffic?
OT Network Security	Edge and OT Network	Is a network level Anti-Malware solution in-line for all traffic? For relevant endpoints, do you have endpoint protection installed?
OT Network Security	Edge and OT Network	How do you control and prevent malicious C&C activities for all traffic?
OT Network Security	Edge and OT Network	How do you mitigate and stop internal and external Recon activities? How do you mitigate against external and internal DDOS attacks?
OT Network Security	Edge and OT Network	Are application based policies and restrictions in place for all traffic?
OT Network Security	Edge and OT Network	What is the decryption coverage for the encrypted traffic, in particular proprietary encryption?

Technology Category	Security Capability	Question
OT Endpoint Security	Users and Data	How do you control user access at the network level?
OT Endpoint Security	Users and Data	Are role based access control and least privilege permissions used to grant access to OT assets?
OT Endpoint Security	Users and Data	Do personnel have unique digital identities, which are used to authenticate to OT assets? (no shared accounts or generic accounts)
OT Endpoint Security	Users and Data	How do you ensure non-sensitive files from all traffic on all ports are sent to an automated malware analysis solution?
OT Endpoint Security	Users and Data	Do you have a baseline for OT endpoint and system hardening?
OT Endpoint Security	Users and Data	Do you do regular patching of key OT systems? Especially the IT systems within OT, such as historians etc.
OT Endpoint Security	Users and Data	Do you have a structure and process around remote access to OT systems?
Continuous Security Monitoring	Logging and Reporting	What is your OT vulnerability identification and management process?
Continuous Security Monitoring	Logging and Reporting	Is network and endpoint data is logged, retained and analysed for cyber security incidents?
Continuous Security Monitoring	Logging and Reporting	Do you have continuous monitoring of anomalous traffic on your OT environment?
Continuous Security Monitoring	Logging and Reporting	Are IOCs found in malicious files automatically turned into network and endpoint prevention updates?
Continuous Security Monitoring	Logging and Reporting	Do you have continuous visibility of IoT devices and their behaviour?
Continuous Security Monitoring	Logging and Reporting	How do you track user activity at the network level?
Supply Chain Management	Suppliers and Contractors	Have key OT suppliers been identified from the perspective of physical assets and data?

Technology Category	Security Capability	Question
Supply Chain Management	Suppliers and Contractors	How do you monitor 3rd Party Engineers in your OT network and prevent network bridging?
Supply Chain Management	Suppliers and Contractors	Have the cyber security risks of OT suppliers been identified and managed?