Cybersecurity Workshop

Simplify Your Cybersecurity Security Roadmap

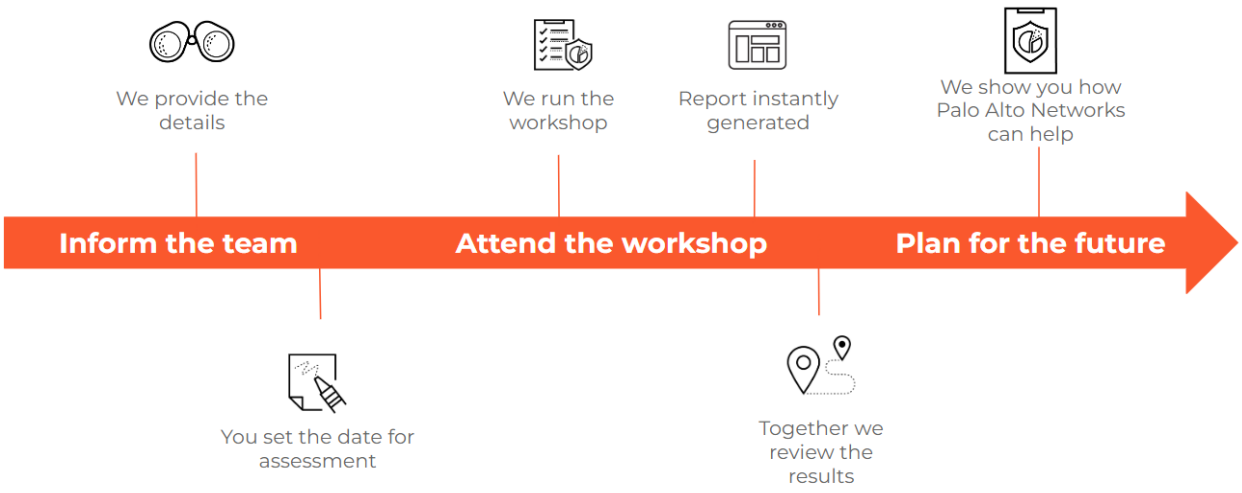
The Cybersecurity Assessment helps develop strategies to protect you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

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 Cybersecurity Assessment can help you reduce risk and improve operational resilience, so you can embrace digital with confidence. We offer a complimentary Cybersecurity 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 Cybersecurity Assessment covers the following technology areas and takes approximately one hour to complete.

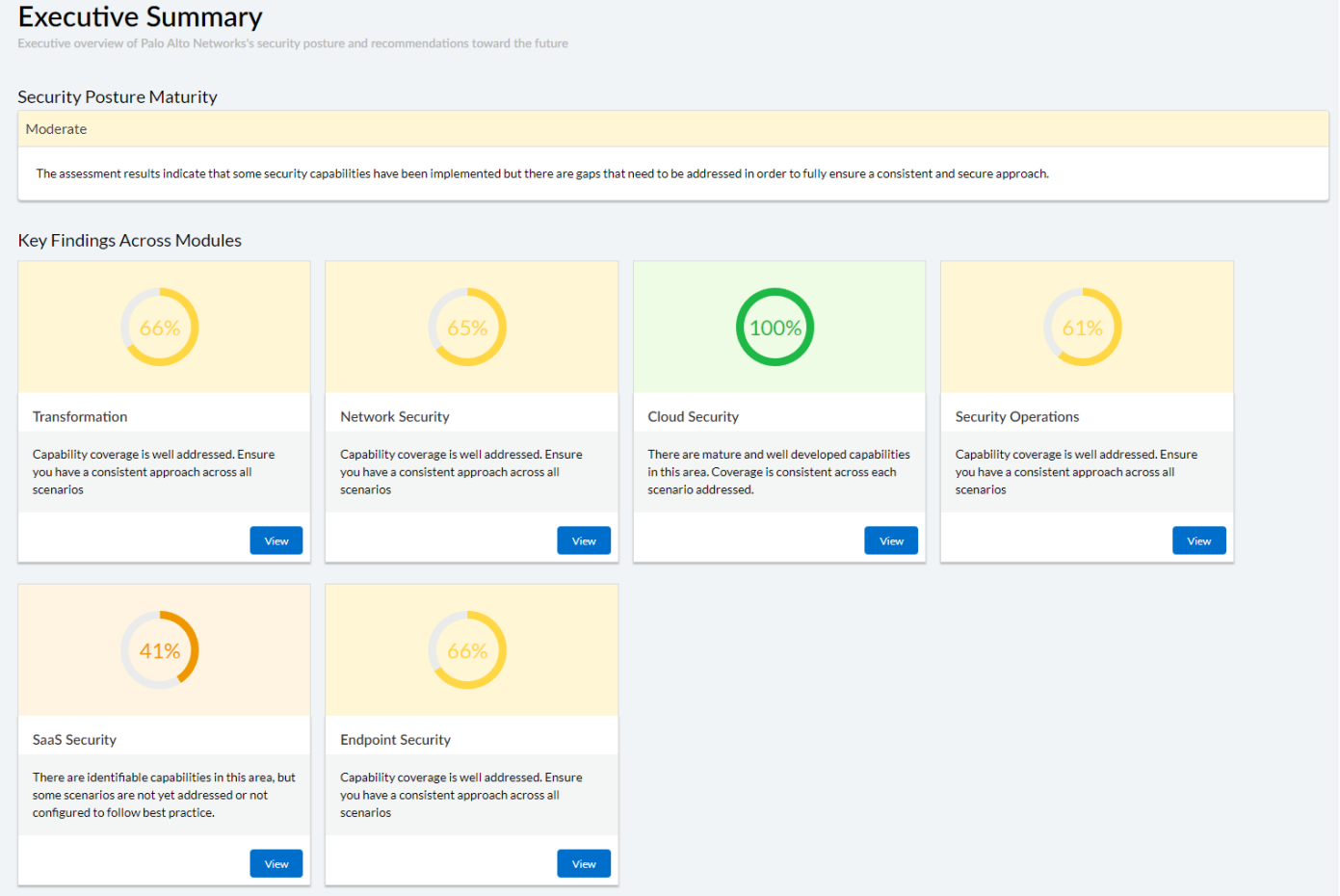
- Cyber Strategy
- Network
- Cloud & SaaS
- Endpoint
- Security Operations



What you can Expect

- An accurate analysis of your current security posture with regards to all the components that make up Cybersecurity - Secure Access Service Edge.
- Enablement of security teams so you may best optimize existing technologies
- Reduction in overall business risk by incorporating new technologies and security controls

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:

- Security Architects
- Network and Infrastructure Operations
- Cloud Dev SecOps
- Helpdesk
- Data Privacy Officer or Cyber Risk Analyst
- SOC Analysts

The workshop comprises the following Security capabilities and questions:

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

Category	Security Capability	Question
Cyber Strategy	Future Priorities	Do you have a vision or a roadmap for technology transformation over the next 3-5 years?
Cyber Strategy	Business Alignment	How aligned are your current security projects to your known business challenges?
Cyber Strategy	Resourcing	Do you have enough resources (people and budget) for your cybersecurity program?
Cyber Strategy	Expert Knowledge	Are you gathering advice and intelligence from Industry experts to help drive your cyber security strategy?
Cyber Strategy	Hybrid work	Is your security portfolio designed to allow for hybrid workers?
Cyber Strategy	Scalable Security	Do your security controls scale with your business? ie More users, devices, locations?
Risk Reduction	Incident Response	In the event of a breach, do you have an incident response plan?
Risk Reduction	Risk of Breach	Have you quantified the risk of a breach?
Risk Reduction	Zero Trust	Is Zero Trust something you are considering and if so, what is driving this decision?
Network Infrastructure	Threat Prevention	Do you have network based threat prevention?
Network Infrastructure	Segmentation	Do you control lateral movement within your environment?

Network Infrastructure	DNS Security	Do you secure your DNS traffic?
Network Infrastructure	IoT Security	How do you protect IoT devices?
Network Infrastructure	Security Coverage and Complexity	How complex is your network security deployment?
Network Infrastructure	Threat Response	How quickly can you identify and respond to network based threats?
Network Application Security	Security Policy	How specific / granular are your security policies?
Network Application Security	Decryption	Are you doing SSL decryption and inspecting for threats?
Network User Security	User Based Policy	Do you apply any user or group specific network policies?
Network User Security	Web Security	Are you monitoring and protecting web activity?
Cloud Infrastructure	Governance and Compliance	Do you have a view of compliance within all of your cloud environments?
Cloud Infrastructure	Vulnerability Management	Are you scanning for vulnerabilities and remediating when found?
Cloud Infrastructure	Infrastructure Protection	How do you detect and remediate cloud infrastructure misconfiguration?
Cloud Infrastructure	Attack surface management	Do you have a view of all your externally visible assets and their risk?
Cloud Application Security	Web Application and API	How do you protect your web applications and API's?
Cloud Application Security	Data Protection	Do you secure cloud based data and datastores?
Cloud Application Security	Code Security	Do you apply any security controls to code being written or deployed?

Cloud User Security	Identity Management	Do you securely manage user, application and infrastructure credentials?
Cloud User Security	Security Impact	What impact does security have on developers and business?
SaaS Application Security	Visibility	Do you know what unsanctioned SaaS applications are being accessed?
SaaS Application Security	Data Management	Can you protect data stored in SaaS applications?
SaaS Application Security	Threat Prevention	Are you able to apply threat prevention to your SaaS applications and data?
SaaS User Security	Control	Can you control which SaaS applications are being used?
SaaS User Security	User Experience	Is there a consistent user experience when accessing SaaS Applications?
Endpoint Infrastructure Security	Threat Prevention	How do you detect and prevent malware, ransomware and viruses on your endpoints?
Endpoint Infrastructure Security	Device Management	Do you apply any security posture assessment of devices either on-premise or remote?
Endpoint Infrastructure Security	Deployment Complexity	How complex is your endpoint security solution? How many agents, impact performance?
Endpoint Application Security	Vulnerability Management	How are you handling vulnerability management for workstations and servers?
Endpoint Application Security	Data Protection	Do you have policy and protection in place for critical and sensitive data?
Endpoint User Security	Behaviour Analysis	Is there any predictive analysis available to show changes in behaviour of a device or user?
Endpoint User Security	User Activity	How are you controlling / monitoring user activity and privilege on your endpoints?
Incident Response	SOC Processes	How defined are your security operations processes?

Incident Response	Level of Automation	How automated are your security operations?
Incident Response	Root cause and forensics	How long does it take to investigate an incident and analyse the issue? (RCA)
Threat Intelligence	Threat Intelligence	Do you leverage threat intel from multiple sources?
Threat Intelligence	Asset Visibility	Does the operations team see all business assets?
Threat Intelligence	Quality of Logs	Is the quality of logs sufficient for incident response and analysis?