Enterprise Security Workshop

Simplify Your Cybersecurity Security Roadmap

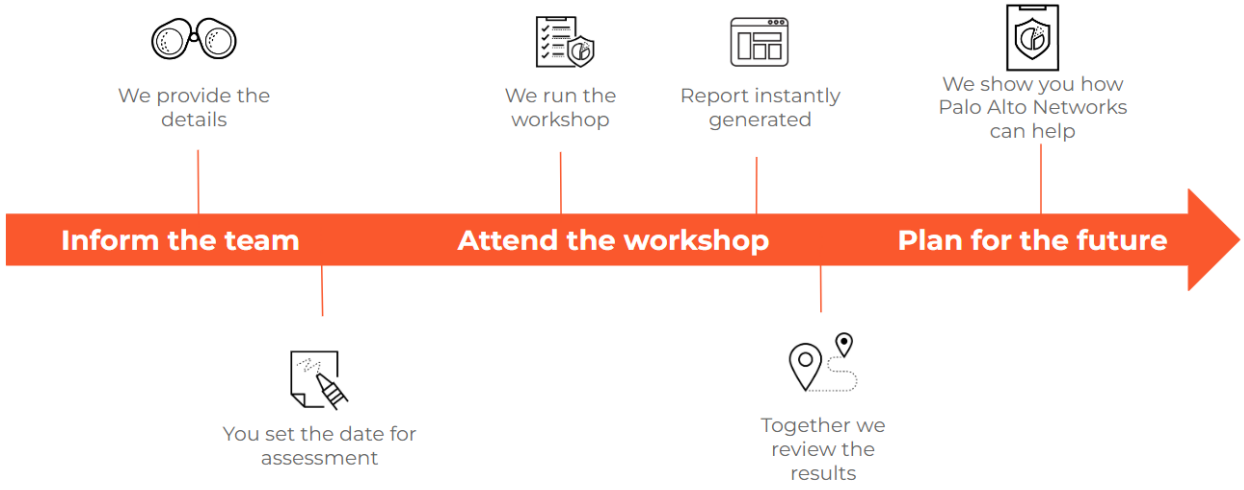
The Enterprise Security Assessment helps develop strategies to protect you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber 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 Enterprise Security Assessment can help you reduce risk and improve operational resilience, so you can embrace digital with confidence. We offer a complimentary Enterprise Security 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 Enterprise Security Assessment covers the following technology areas and takes approximately four hours to complete.

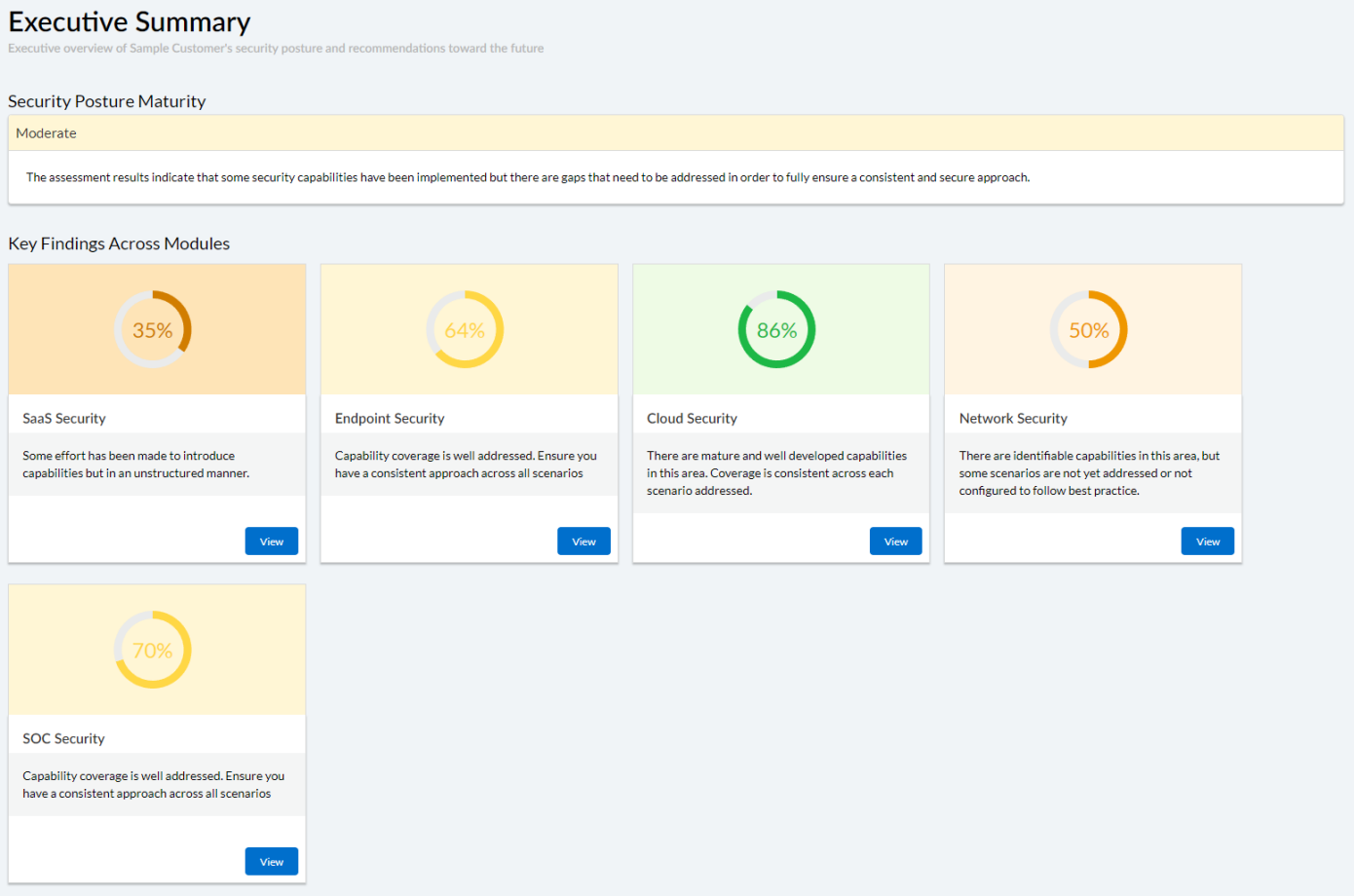
- Network
- Cloud & SaaS
- Endpoint
- Security Operations



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
Network Security	Anti-Malware	Is a network level Anti-Malware solution in-line for all traffic?
Network Security	Anti-Spyware	How do you control and prevent malicious command-and-control activities?
Network Security	Sandboxing	How do you ensure non-sensitive files from all traffic on all ports are sent to an automated malware analysis solution?
Network Security	Automated Malware Analysis	Are IOCs found in malicious files automatically turned into network and endpoint prevention updates?
Network Security	Content Updates	How often do you perform content updates for threat prevention capabilities (AV, IPS, C2, DNS, URL)?
Network Security	Application Control	Is application access controlled in network security policies?
Network Security	Application Visibility	Can you identify applications in network traffic logs?
Network Security	Unidentified Traffic	How are unauthorized and unidentifiable applications identified and controlled at the network level? (e.g. evasive, tunneling, remote-access, unknown, ...)?
Network Security	Asset Discovery	Do you maintain an active list of assets within your network? Is it automated or manual?
Network Security	Compliance Standards	How well do you adhere to a compliance standard? NIST, ISO27001, CIS etc
Network Security	Email Security	How do you prevent malicious emails from reaching the end user for both corporate and personal email?

Category	Security Capability	Question
Network Security	File Transfer	How is the transfer of files controlled in both download and upload direction?
Network Security	Sensitive Data Visibility	Do you identify sensitive content in network traffic?
Network Security	Sensitive Data Control	Do you prevent sensitive content from leaving the network?
Network Security	Decryption Coverage	What is the decryption coverage for the encrypted traffic? Is there any SSL Decryption (inbound or outbound) applied to traffic.
Network Security	Decryption Control	How do you control traffic that can not be decrypted due to technical reasons (certificate pinning, unsupported ciphers, ...)?
Network Security	Invalid Certificates	How do you prevent encrypted traffic to websites with invalid or expired certificates?
Network Security	IOT Segmentation	How are you securing and segmenting IOT devices?
Network Security	Out of Band Management	How do you restrict access to network infrastructure management?
Network Security	DNS Restrictions	Do you restrict outbound DNS and DNS forwarders to an approved list?
Network Security	DNS Tunneling	How do you inspect DNS traffic for tunneling activity?
Network Security	DNS DGAs	Are you able to detect and block malicious domains created by domain generation algorithms? (DGAs)
Network Security	DNS Sinkhole	Do you sinkhole suspicious DNS queries to validate the internal source IP?
Network Security	DoS	How do you mitigate DOS attacks?
Network Security	Reconnaissance	How do you mitigate and stop internal and external Recon activities?

Category	Security Capability	Question
Network Security	Centralized Logging	Are logs forwarded to a central logging repository for security monitoring purposes?
Network Security	Log Retention	What is your log retention period for proactive monitoring and behavioral analysis purposes?
Network Security	Log Storage	Do you backup logs to internal/external storage to meet compliance requirements around long-term log retention?
Network Security	Segmentation	How do you segment your network environment up to layer 7 to prevent lateral threat movement?
Network Security	Micro Segmentation	Have you implemented microsegmentation in any network segments?
Network Security	Multi-Factor Authentication	Is Multi-Factor Authentication in place to control access to critical systems, applications and data?
Network Security	User Visibility	How do you track user activity at the network level?
Network Security	User Control	Is access to systems based on user identity controlled by a firewall or other network device?
Network Security	Behavioral Analytics	Are you looking for abnormal activities of machines and users who are accessing company digital assets?
Network Security	Vulnerability Discovery	Do you conduct regular pentesting of your environment?
Network Security	Vulnerability Management	Is a network-level Vulnerability protection solution in line for all traffic?
Network Security	Vulnerability Remediation	Do you have a process to remediate vulnerabilities in infrastructure as they occur?
Network Security	Dynamic Block Lists	How do you automatically block known malicious IP Addresses and URLs, based on threat intelligence from third-party feeds?
Network Security	Credential Theft Prevention	How do you prevent Credential Phishing attempts?

Category	Security Capability	Question
Network Security	URL Filtering	Do you block known bad URLs across all ports, or use a Proxy for HTTP and HTTPS traffic only?
Network Security	URL Logging	Do you alert, log and correlate on known-bad, unknown and IP-based URLs?
Cloud Security	Anti-Malware	How do you detect and remediate malware at-rest within your public cloud environments?
Cloud Security	Anti-Spyware	How do you control and prevent malicious command-and-control activities?
Cloud Security	Sandboxing	How do you ensure non-sensitive files from all traffic on all ports are sent to an automated malware analysis solution?
Cloud Security	Content Updates	How often do you perform content updates for threat prevention capabilities (AV, IPS, C2, DNS, URL)?
Cloud Security	Apps and API	How do you protect your web applications and application APIs against network-based attacks?
Cloud Security	Anti-Ransomware	How do you prevent encryption of systems by ransomware attacks?
Cloud Security	Application Control	Is access over the network controlled via a least-privilege policy?
Cloud Security	Application Visibility	Can you identify applications in network traffic logs?
Cloud Security	Unidentified Traffic	How are unauthorized and unidentifiable applications identified and controlled at the network level? (e.g. evasive, tunneling, remote-access, unknown, ...)?
Cloud Security	Asset Discovery	How do you discover and manage your assets running inside your public cloud environments?
Cloud Security	Asset Change History	How do you track all historical changes made to them?
Cloud Security	Attack Surface Management	How do you keep track of all sanctioned and unsanctioned public-facing assets?

Category	Security Capability	Question
Cloud Security	CI/CD Security	Do you have security embedded into the CI/CD pipeline to automate assessments and remediation?
Cloud Security	SOC Integration	Do you have integration between your cloud security capabilities and SIEM/SOAR solutions?
Cloud Security	Dynamic Threat Prevention Coverage	Does your cloud security infrastructure automatically scale to support increases/decreases in workloads and asset coverage?
Cloud Security	Cloud Infrastructure Code	How do you detect and remediate cloud infrastructure misconfiguration?
Cloud Security	IaC Templates	How do you detect and remediate IaC template misconfiguration?
Cloud Security	Assurance Monitoring	Do you have continuous compliance assurance monitoring in place for your cloud environments?
Cloud Security	Governance	Do you have a centralized view of risk across your cloud and microservices architectures?
Cloud Security	Data Classification	How do you identify if sensitive content is being stored in your cloud environments?
Cloud Security	Data Leakage Prevention	How do you identify if sensitive content is being shared publicly or inappropriately through your cloud environments?
Cloud Security	Data Encryption	How do you verify and enforce encryption of sensitive data in-transit and at-rest?
Cloud Security	DNS Restrictions	Do you restrict outbound DNS and DNS forwarders to an approved list?
Cloud Security	DNS Tunneling	How do you inspect DNS traffic for tunneling activity?
Cloud Security	DNS DGAs	Are you able to detect and block malicious domains created by domain generation algorithms? (DGAs)
Cloud Security	DNS Sinkhole	Do you sinkhole suspicious DNS queries to validate the internal source IP?

Category	Security Capability	Question
Cloud Security	Centralized Logging	Are logs forwarded to a central logging repository for security monitoring purposes?
Cloud Security	Log Retention	What is your log retention period for proactive monitoring and behavioral analysis purposes?
Cloud Security	Log Storage	Do you backup logs to internal/external storage to meet compliance requirements around long-term log retention?
Cloud Security	Multi Cloud Management	How do you manage resources across public cloud providers?
Cloud Security	Segmentation	How do you segment your network environment up to layer 7 to prevent lateral threat movement?
Cloud Security	Micro Segmentation	Have you implemented microsegmentation in any network segments?
Cloud Security	MFA	Is Multi-Factor Authentication in place to control access to critical systems, applications and data?
Cloud Security	User Control	How do you control user access and monitor activity towards internal and external systems and applications?
Cloud Security	User Privilege	How do you maintain visibility and control over the effective user privileges across your cloud environments?
Cloud Security	Behavioral Analytics	Do you leverage behavioral analysis to detect advanced attacks?
Cloud Security	Vulnerability Discovery	Do you leverage behavioral analysis to detect advanced attacks?
Cloud Security	Pen Testing	Do you conduct regular pentesting of your environment?
Cloud Security	Vulnerability Remediation	How fast are you able to remediate discovered vulnerabilities?
Cloud Security	URL Filtering	Do you inspect URLs and web traffic for content, malware, corporate usage reasons?

Category	Security Capability	Question
Cloud Security	URL Logging	Do you alert, log and correlate on known-bad, unknown and IP-based URLs?
SaaS Security	Anti-Malware	How do you protect from malware at-rest within SaaS applications?
SaaS Security	Sanctioned and Unsanctioned Access	How is access to sanctioned, tolerated and unsanctioned SaaS applications monitored and controlled?
SaaS Security	Sanctioned Applications	Do you maintain a list of Sanctioned, Unsanctioned and Tolerated SaaS applications for your enterprise?
SaaS Security	Policy Enforcement	How do you globally enforce your SaaS governance and policies?
SaaS Security	Content Storage Control	How do you identify if sensitive content is being stored in your sanctioned SaaS applications?
SaaS Security	Content Sharing Control	How do you identify if sensitive content is being shared publicly or inappropriately in your sanctioned SaaS applications?
SaaS Security	Data Leakage Prevention	How do you control transfer of data into and out of key SaaS applications?
SaaS Security	Centralized Logging	Are logs forwarded to a central logging repository for security monitoring purposes?
SaaS Security	Log Retention	What is your log retention period for proactive monitoring and behavioral analysis purposes?
SaaS Security	Log Storage	Do you backup logs to internal/external storage to meet compliance requirements around long-term log retention?
SaaS Security	User Activity Reporting	How do you report on and control user activity within SaaS applications?
SaaS Security	MFA	Is Multi-Factor Authentication in place to control access to SaaS applications?
Endpoint Security	Exploit Prevention	How do you prevent exploits on physical and virtual Windows, Linux and MacOS systems?

Category	Security Capability	Question
Endpoint Security	Anti-Malware	How do you prevent malware presence and execution on physical and virtual systems?
Endpoint Security	Automated Malware Analysis	Are Indicators of Compromise (IOCs) found in malicious files automatically turned into network and endpoint prevention updates?
Endpoint Security	Periodic Scanning	Do you perform periodic scanning of windows hosts?
Endpoint Security	Anti-Ransomware	How do you prevent encryption of systems by ransomware attacks?
Endpoint Security	Restrict Operations	How do you control and restrict operations on endpoints? (command line execution, processes, activities from logical drives, activities from hardware locations, etc.?
Endpoint Security	Process Spawning	How do you prevent unwanted process spawning activities? (powershell launching command)
Endpoint Security	Content Updates	How do you maintain your endpoint security updates?
Endpoint Security	Policy Protection	How do you detect policy violations?
Endpoint Security	Agent Protection	Are you able to prevent unauthorized agent shutdown actions?
Endpoint Security	Application Control	Do you have full visibility into executable applications and the ability to limit execution of unwanted applications?
Endpoint Security	Asset Discovery	How do you discover and manage endpoints across the organization?
Endpoint Security	Asset Changes	How do you track asset configuration changes?
Endpoint Security	Application Inventory	How do you discover and manage installed applications for all workstation and server endpoints?

Category	Security Capability	Question
Endpoint Security	Detect and Respond	How do you create and deploy custom detection policies to the endpoints and servers?
Endpoint Security	BYOD	How do you secure your resources while still allowing BYOD policies?
Endpoint Security	File Search and Destroy	How do you eradicate malicious or suspicious files from endpoints as part of a breach mitigation workflow?
Endpoint Security	Data Classification	Have you implemented a data classification methodology?
Endpoint Security	Data Encryption	How do you verify and enforce encryption of sensitive data in-transit and at-rest?
Endpoint Security	USB Device Control	Do you scan, inspect or prevent the use of removable drives?
Endpoint Security	Host Based Firewall	Do you leverage a host-based firewall to control network access to and from endpoints?
Endpoint Security	Forensic Logging	How do you collect and store forensic data from the endpoints and servers?
Endpoint Security	Centralized Logging	Are logs forwarded to a central logging repository for security monitoring purposes?
Endpoint Security	Log Stitching	Are you performing log stitching for incident analysis with network and other log sources?
Endpoint Security	Privileged Accounts	How do you control privilege account access on endpoints?
Endpoint Security	Behavioral Analytics	Do you leverage behavioral analysis to detect advanced attacks?
Endpoint Security	Vulnerability Discovery	How do you discover and manage vulnerabilities on managed endpoints?
Endpoint Security	Pen Testing	Do you conduct regular pentesting of your environment?

Category	Security Capability	Question
Endpoint Security	Unsupported OS	How do you monitor and protect unsupported OS versions?
SOC Maturity	Security Team	How many people are in your Security Team that work alerts?
SOC Maturity	Team Maturity	How experienced are the people that work alerts? How often do they receive technically relevant training?
SOC Maturity	Workload	Roughly how many tickets does your Security Team process per day on average? How many of those tickets are security alerts?
SOC Maturity	Coverage	Do you have 24/7 coverage and how do you achieve it?
SOC Maturity	Alert Handling	Do you know how many alerts your Security Team can handle per day?
SOC Maturity	Alert Validation	Do you know the average length of time to validate a security alert?
SOC Maturity	Alert Deficit	Do you track the number of alerts that were not triaged the same day? (alert deficit)
SOC Maturity	Automated Alert Prioritization	Do you use automation to triage, prioritize and respond to alerts, if so which tools?
SOC Maturity	Security Tool POCs	How frequently do you support POCs/POVs for new security tools? How long does the average POC take? Roughly how much effort does it require?
SOC Maturity	Security Tool Onboarding	What is your strategy and process to onboard new security tools and if so what are they?
SOC Maturity	KPI Tracking	Do you have the capability to track KPIs or metrics in your Security Team to measure efficiency and effectiveness? If so, what are a few of your most useful metrics that you track.
SOC Maturity	Incident Response Timing	Do you have the capability to track the time between your IR phases (identification, investigation, mitigation)? If so, what are they?

Category	Security Capability	Question
SOC Maturity	Threat Intelligence	Do you leverage threat intelligence feeds from external sources? If so, how?
SOC Maturity	Correlation	Do you correlate security events across different enforcement points and other relevant logs sources? If so, how?
SOC Maturity	False Positives	Do you have a process to eliminate false positives?
SOC Maturity	Public Cloud	Do you have public cloud instances? If so, how do you monitor them for cybersecurity events?
SOC Maturity	Behavioral Analytics	Do you have the capability to identify threats based on behavior-based analysis?
SOC Maturity	Monitored Alerts	Do you have a defined process to determine which alerts end up in the SOC's security monitoring queue?
SOC Maturity	Threat Hunting	Does your SOC perform threat hunting? If so, what tools do you use, in what frequency do you hunt, and what sort of things do you hunt for?
SOC Maturity	Incident Response Process	Do you have a documented process to respond to cyber security incidents?
SOC Maturity	Detect and Respond	Do you use forensic or detection and response tools predominantly for incident handling?
SOC Maturity	IOC Research	Do you perform research on IOCs seen in your environment (ip addresses urls, files, registry keys, OS artifacts)?
SOC Maturity	IOC Comparison	Do you compare IOCs and Intel between your organization, your industry and the global threat space?
SOC Maturity	Forensic Logging	Do you preserve forensic evidence from the network, endpoint and cloud and re-use them? And if so how?
SOC Maturity	Host Isolation	Do you have the capability to isolate suspicious hosts and if so what tools do you use?
SOC Maturity	Business Continuity	Do you ensure that business critical systems/services are not inadvertently disrupted as a result of security incident response activities? How do you ensure this?

Category	Security Capability	Question
SOC Maturity	Incident Review	Do security teams review activities of incidents and share knowledge gained to other team members? If so, how? Summarizing information as context in future investigations is key to creating operational efficiency and increasing accuracy of less-skilled team members.
SOC Maturity	Playbooks	Are security teams empowered to create new custom detections against newly found tactics, techniques and procedures (TTPs) to detect future attacks based on incident finding on your endpoints network and cloud, and if so, how?
SOC Maturity	Feedback and Knowledge Sharing	Do you have a process in place to update your security controls against future attacks based on incident findings on your endpoints, network and cloud? And if so how?
SOC Maturity	Alert Fidelity	Do you measure the fidelity and prioritization of alerts that are escalated to incidents and if so how? (true positive vs false positive)