Modern SOC Assessment

Transform the SOC to be Machine-led, Human Empowered

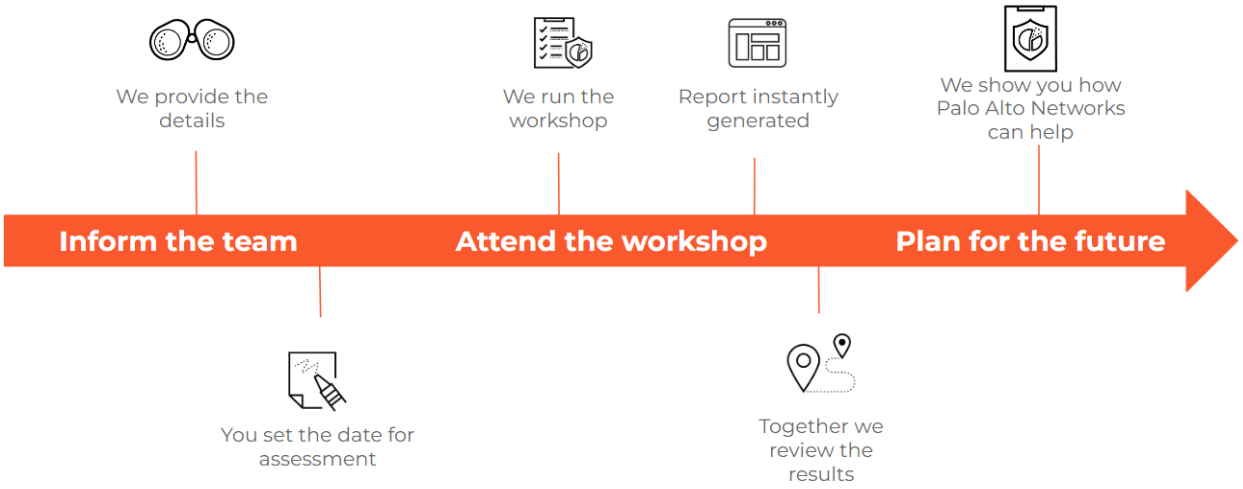
The Security Posture Assessment (SPA) supports your cybersecurity planning and strategy by providing in-depth, current state analysis and expert-level recommendations for your security operations environment.

Overview

Organisations preparing to transform security operations and leverage the best of AI, Automation and a “shift right” approach need to gain an understanding of their current capabilities and identify any areas that require attention before applying new technologies. Leverage the Modern SOC Assessment to get a view of both the log generation and log analysis engines within your infrastructure and determine the most effective next steps and priorities.

The Modern SOC Assessment covers the following technology areas and takes between 90-120 minutes to complete.

- Network Monitoring
- Endpoint Detection & Response
- SIEM
- SOAR
- Attack Surface Management
- Identity Threat Detection and Response
- Threat Intelligence Management
- Cloud Service Monitoring



What you can expect

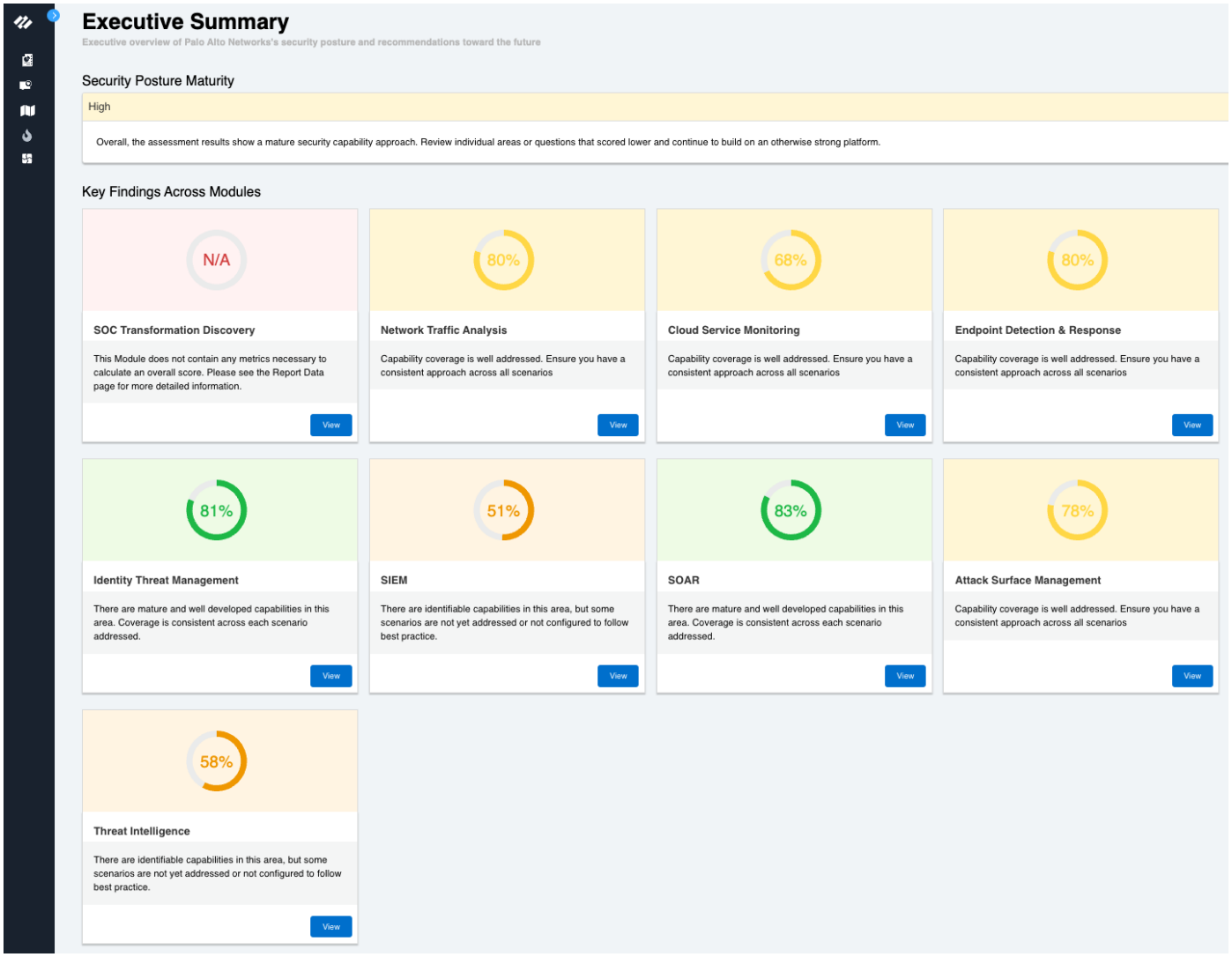
- An overview of the components that make up a Modern SOC environment
- A high level, customisable roadmap of priorities
- Recommendations for improvements and the business benefits of each

Who should attend the workshop

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

- Network and Infrastructure Operations
- Security Operations Dev SecOps
- Data Privacy Officer or Cyber Risk Analyst

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



The workshop comprises the following Security capabilities and questions:

Technology Category	Question	Question Background
SOC Transformation Discovery	Is your SOC currently internal, outsourced or a combination?	Understanding the structure of the current operations process helps when trying to address challenges and identity responsibilities.
SOC Transformation Discovery	How many people in your Security Team are working on alerts?	This is anyone who is directly involved in receiving, sorting and allocating alerts and incidents.
SOC Transformation Discovery	How many people in your Security Team are working on content creation? E.g. onboarding of new data source, creating log parsers, creating of correlation rules?	This is anyone who is directly involved in onboarding new data sources and creating new security correlation rules.
SOC Transformation Discovery	Do you have the capability, or a team, to conduct threat hunting?	It's important to be as proactive as possible when it comes to threat analysis and once a SOC reaches a level of automation for repetitive tasks, team members should be upskilled and empowered to threat hunt in order to stay ahead of their adversaries.
SOC Transformation Discovery	What is the main constraining factor(s) you have currently in your SOC?	For Example: Cost overrun on your current SIEM / Data Aggregation System, difficulty introducing/maintaining security analytics like UEBA or NTA, SOC analysts burning out or being overwhelmed, difficulty in scaling your SOC to meet the security challenges of the future with the tools and number of people you have now, being reluctant to automate alerts as you're worried by false positives.
SOC Transformation Discovery	Do you measure your security operations? Can you measure your MTTR? (Mean time to Resolution) If so, what is it?	Examples include MTTR, Response times, staff load, % of alerts from total logged data.
SOC Transformation Discovery	What is the overall size of your organization? How many staff, endpoints, devices?	This will help determine the scope and coverage your security operations in order to effectively scale with the business.
SOC Transformation Discovery	How many tools do your SOC analysts use in their daily work?	Many organizations have found the need to invest in multiple tools in order to operate their SOC. As threats increase in speed and frequency, businesses are often aiming to simplify and consolidate the number of tools to allow analysts and operators to work more efficiently.

Technology Category	Question	Question Background
SOC Transformation Discovery	Do you know the current data ingestion quantity in the SIEM? (In EPS and GB/Day ingestion metrics if possible)	This helps to understand the size and scope of your data, potential impact on throughput and costs incurred. EPS (Events per Second) and GB (Gigabit per day)
SOC Transformation Discovery	What are the current data log sources ingested by the SIEM?	It's important to ensure logging is done as widely as possible across the organization to reduce gaps in visibility.
SOC Transformation Discovery	How many alerts are generated and how many become incidents - ie what % and how many?	Generally it's assumed that only a small percentage of the overall log volume results in an alert, and similarly a smaller amount still that become incidents. Understanding these metrics is useful in ensuring security operations are appropriately staffed, and that security controls are effective in most cases.
SOC Transformation Discovery	Are you using a SIEM exclusively for security data? Is it on-premise or cloud based?	Some organizations have cross functional use cases for SIEM data where non security sources are ingested and dashboards and reporting meets a variety of outcomes.
SOC Transformation Discovery	Is your logging data subject to any overseas or cloud hosted data compliance issues or requirements?	When considering any new technical solutions and platforms its prudent to check for data regulations that may apply.
Network Traffic Analysis	Do you have network based threat and traffic inspection?	It is crucial to have network level visibility for all traffic and threat and ensure that any detected anomalies are acted upon.
Network Traffic Analysis	Can you identify applications and users in network traffic logs?	Being able to see detailed application and user information can help build a strong security policy set and provides the necessary visibility for the security team to take action.
Network Traffic Analysis	Are you doing SSL decryption and inspecting for threats?	SSL is commonly applied to web traffic and without decryption and a security solution to inspect it, there is limited visibility into the threat landscape.
Network Traffic Analysis	Are you monitoring and protecting web activity?	External facing web app/services are very common to most business and easily to be targeted as an attack surface.
Network Traffic Analysis	Are you able to detect unusual network behavior in your environment?	Sophisticated attacks will be aware of triggering alerts and focus on staying hidden and affecting systems over a long period of time. Having the tools to detect unusual activity, regardless of how minor, allows the SOC team to stay ahead of the threat.
Network Traffic Analysis	Do you control lateral movement within your environment?	Lateral movement prevention is critical in terms of resilience and damage control.

Technology Category	Question	Question Background
Network Traffic Analysis	Are your network threat signatures updated regularly and consistently across your organization?	It's important to have a complete and consistent approach to threat updates as attackers often leverage CVE data to exploit organizations.
Network Traffic Analysis	How quickly can you isolate and remediate a network based threat?	Network based threats often spread quickly so it makes an impactful difference whether you can isolate and remediate quickly.
Cloud Service Monitoring	Are you collecting flow logs and alert data from your cloud assets?	Cloud assets are often more complex and dynamic than traditional on-premises assets which can lead to gaps in visibility. It is essential to identify all assets that need to be protected and the threats they may face.
Cloud Service Monitoring	Can you determine the level of compliance across your cloud assets?	Compliance risks are risks that arise from an organization's failure to comply with applicable laws, regulations, and industry standards. Compliance risks can be particularly significant for cloud assets, as cloud providers are often subject to different compliance requirements than on-premises environments.
Cloud Service Monitoring	Are you tracking vulnerabilities in code and infrastructure?	Vulnerabilities in code and infrastructure can be exploited by attackers to gain access to systems and data, or to disrupt operations. Identifying vulnerabilities in weak code and development infrastructure identifies risks for prioritization of remediation.
Cloud Service Monitoring	How do you protect your web applications and API's?	Web applications and APIs are often complex and difficult to secure, and they can provide attackers with a way to gain access to sensitive data or systems. Robust capabilities for securing and monitoring web applications and APIs is essential for any organization that wants to protect its data.
Cloud Service Monitoring	How do you respond to security events for your cloud environments and assets?	If the SOC is involved in events that originate from Cloud based resources, are the incidents handled any differently? Is there another team that handles these events?
Endpoint Detection & Response	Do you have EPP and EDR capabilities deployed currently?	An endpoint protection platform (EPP) is usually the fundamental of security and Endpoint Detection and Response (EDR) provides quick remediation capability which usually determines damage level for an intrusion.
Endpoint Detection & Response	How do you discover and manage vulnerabilities and threats on endpoints?	Most organizations will have a vulnerability discovery tool and process in place and a process to determine how vulnerabilities are actioned/mitigated.

Technology Category	Question	Question Background
Endpoint Detection & Response	How do you prevent the spread and blast radius of threats that impact your endpoints?	If malware passes into the network and gains a foothold, it's important to be able to restrict movement across subnets and within business units in order to minimise the impact.
Endpoint Detection & Response	Do you have the ability to perform investigations on endpoint remotely without using additional tools?	Remote endpoint investigations can be performed more quickly and efficiently than on-site investigations. This is because SOC analysts do not have to travel to the endpoint location, which can save a significant amount of time and resources. The flexibility can be especially beneficial for organizations with a global workforce or for organizations that need to respond to security incidents outside of normal business hours.
Endpoint Detection & Response	Do you leverage behavioral analysis to detect advanced attacks?	Being able to define normal and abnormal traffic flows assists in finding otherwise hidden attack vectors and strategies.
Endpoint Detection & Response	Do you preserve forensic evidence from the endpoints and re-use them? And if so how?	When threats are found on systems inside the organization, is evidence available to ensure a repeat attempt to breach is prevented?
Identity Threat Management	How do you control user account access and activity on your endpoints?	Both privilege escalation and overly permissive account access can lead to a threat actor obtaining access to otherwise restricted resources. Only provide elevated permissions where needed and ensure privileged accounts are audited.
Identity Threat Management	Is Multi-Factor Authentication in place to control access to critical systems, applications and data?	MFA should be used where possible as it gives an additional layer of protection to legitimate credentials. Ideally this would be enabled for corporate device access, SaaS and cloud applications and critical assets hosted within the datacenter.
Identity Threat Management	Do you securely manage user, application and infrastructure credentials?	Credential leakage is of low cost to an attacker and critical in all compliance models.
SIEM	Do you have any data sources that are excluded from the SIEM?	If there are any data sources that are excluded from the SIEM, then the SOC will not have visibility into the activity on those sources. This could mean that the SOC is missing important information that could help to identify and respond to threats.
SIEM	Is the quality of logs sufficient for incident response and analysis?	If the quality of logs is poor, then there may be difficulty identifying suspicious activity. Poor quality logs may be incomplete, inaccurate, or difficult to understand. In addition, poor quality logs can make it difficult for investigation and response because the responder may not have enough information to understand the scope of the threat or to determine how to mitigate it.

Technology Category	Question	Question Background
SIEM	How do you normalize logs before feeding them into your SIEM? How long does it take to operationalize?	Log normalization is the process of converting logs from different sources into a consistent format, making them easier to read and analyze. This is important because logs from different sources can vary widely in their format, structure, and content. If logs are not normalized, it can be difficult for a SIEM to parse and analyze them effectively. This can lead to missed alerts and increased risk of security incidents. The speed to complete this will determine how fast you can put in place detection for a threat thus affecting the MTTD matrix.
SIEM	How do you test your SIEM rules and alerts to ensure their effectiveness?	SIEM rules and alerts are used to identify suspicious activity in security logs. If the SIEM rules and alerts are not effective, then the responders may not be able to detect security incidents in a timely manner, or may be overwhelmed by the number of false positives generated by the SIEM.
SIEM	How often do you review your correlation rules?	Correlation rules needs to be tuned frequently to ensure that they are up to date to detect advance threats in your environment.
SIEM	Are you able to add a new IOC detection to the SIEM without creating complex correlation rules, and automatically perform retrospective analysis?	IOC hunting/retrospective analysis is a day-to-day job in SOC. It requires a lot of overhead if correlation rules are required to detect the ever changing IOC.
SIEM	Are your existing SIEM use cases clearly documented?	It is essential to plan and document SIEM use cases for ensuring that the SOC is adequately protecting the organization from known and emerging threats. Well-documented use cases can help to ensure that the SOC is prioritizing and responding to the most critical threats first and in a timely manner. Mature SOCs will typically have a well-defined set of documented use cases that are regularly reviewed and updated.
SOAR	Are you utilizing AI features in your platforms to improve security posture?	AI can be a powerful tool for improving the effectiveness and efficiency of security analytics. This frees analysts to work on more proactive and innovative tasks while leaving AI to do the more menial tasks and analysis. AI features in its platforms is likely to have a more effective and efficient security posture .
SOAR	Do you leverage a SOAR platform to correlate security events across different enforcement points and other relevant logs sources?	Security logs from network Firewalls, Endpoints, Domain Controllers etc should all be sent to the SOC who should have appropriate tools or knowledge across each area of the team to correlate them efficiently.

Technology Category	Question	Question Background
SOAR	Do you have a defined process to determine which alerts end up in the SOC's security monitoring queue?	There are specific alerts that a SOC ideally wants to monitor in order to stay efficient and catch what is important. Either a too low or a too high number of use cases that are being monitored could result in either missing on important events or getting overwhelmed. A process to define which alerting use cases to monitor needs to be in place.
SOAR	Do you have any automation and orchestration capabilities in your SOC?	Automation and orchestration can help SOC analysts to automate repetitive tasks, such as triage and investigation, which can free up their time to focus on more complex and high-value tasks. This can lead to improved efficiency and effectiveness in the SOC.
SOAR	Do you know the average length of time to validate a security alert? How long does it take to qualify an event of interest?	Understanding the average time for alert triage will identify if efficiencies can be gained, the level of expertise can affect these times and so too can the number of daily repetitive alerts (false positives) that should be removed through policy updates that are not yet implemented
SOAR	How automated is your incident handling process?	A process should exists to identify alerts and incidents as fast as possible.
Attack Surface Management	Do you have a view of all your assets, particularly externally facing assets and their risk profile?	Is a solution is in place that allows automated asset discovery, for asset management and unknown device discovery? A tool/process should exist that allows discovery and mitigation of unwanted assets (e.g. devices plugged into network, virtual machines started). Discovery should be done at the network or cloud infrastructure level.
Attack Surface Management	Are you detecting threat exposure activity with your external assets?	External assets are often at a higher risk of attack than internal assets because they are more exposed to the public internet. Attackers can target external assets through a variety of methods, such as phishing attacks, malware distribution, and denial-of-service attacks. By logging threat and traffic inspection for external assets, you can gain valuable insights into the threats that are targeting their organization.
Attack Surface Management	Are you correlating threat logs for external assets with other log sources?	It is essential to have a comprehensive view of all security threats to your organization, including those that may be targeting external assets. By correlating threat logs from different sources, you can identify patterns and trends that may not be visible in any one source on its own. This can help you to more quickly and effectively detect and respond to threats.

Technology Category	Question	Question Background
Attack Surface Management	How are you protecting your externally accessible assets?	It is important to protect externally accessible assets because they are at a higher risk of attack than assets that are not accessible from the outside.
Attack Surface Management	Are you monitoring remote worker networks and assets?	Remote workers are often more vulnerable to cyberattacks than traditional office workers because remote workers may be using their own personal devices and networks, which may not be as secure as the organization's corporate assets and network. Monitoring remote worker networks and assets can help to identify and respond to threats before they cause significant damage. This can be done by collecting and analyzing data from remote worker devices and networks, such as firewall logs, network traffic logs, and endpoint security logs.
Attack Surface Management	How do you respond to threats from outside your organization?	Mature SOCs will have a well-defined process for responding to external threats, which will include steps to identify, contain, eradicate, and recover from the threat. It helps to ensure that the SOC is aligned with the organization's overall security posture and risk tolerance.
Threat Intelligence	Do you leverage threat intelligence feeds from external sources? If so, how?	A threat intelligence feed is a real-time, continuous data stream that gathers information related to cyber risks or threats. These usually focuses on a single area of interest, such as unusual domains, malware signatures, or IP addresses associated with known threat actors. It's important to have a range of sources in order to validate the accuracy and relevance of a particular threat.
Threat Intelligence	Can you proactively perform Threat Hunting in your environment based on threat intelligence received?	Active Threat hunting is an essential activity for a modern SOC. Threat hunting is the art of searching for the traces attackers leave behind in an IT environment, usually before any alerts of their activities are generated by security devices. This is due to the custom nature of sophisticated attacks and that security teams understand their network, gaps and potential vulnerabilities that allow them to identify issues. The best threat hunters use threat intelligence, custom tools or threat hunting products. Threat hunting ranges from artifact searches (easy to do and easy to evade) to searching for Tactics, Techniques and Procedures (behaviors - hard to find but hard to evade)

Technology Category	Question	Question Background
Threat Intelligence	Do you compare IOCs and Intel between your organization, your industry and the global threat space?	Modern SOCs do not to work in a silos but to also have an eye on what is going on on the outside world. This in order to have a better understanding of the adversaries or campaigns that might be targeting the organization
Threat Intelligence	Can you identify behavioral-based IOCs (BIOC) seen in your environment and apply it to your threat intelligence?	A prevention-based approach requires indicators of attack to be analysed and threat response data should be added to enforcement points in order to mitigate compromise before it occurs.