Network Workshop

Simplify Your Network Security Roadmap

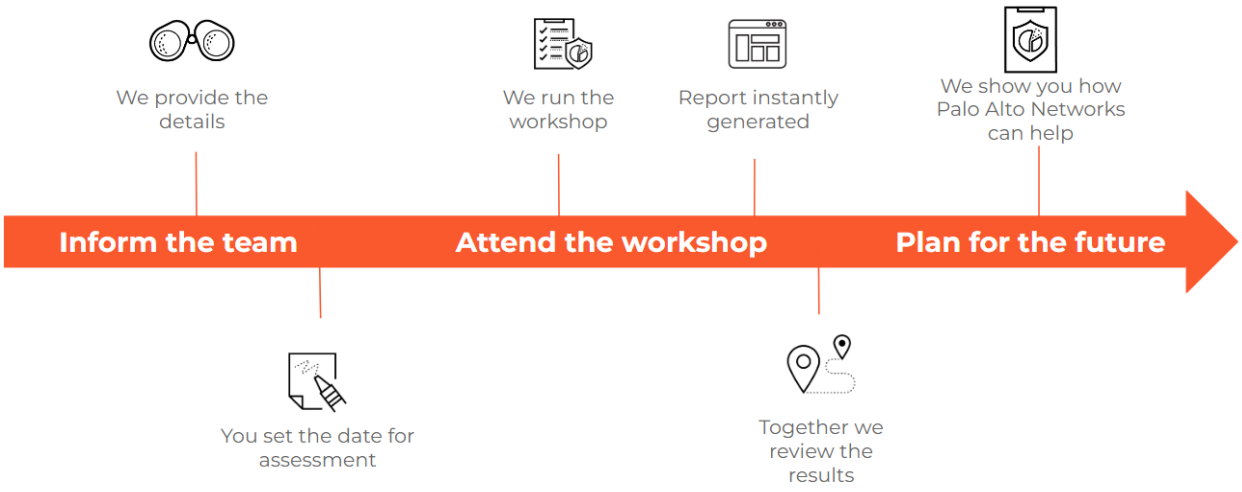
The Network Assessment protects you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

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

- Internal Core
- DMZ
- User Internet Access
- Branch Office
- 3rd Party Access
- Data Centre
- Remote User Access



What you can Expect

- An accurate analysis of your current security posture.
- Enablement of security teams so you may best optimize existing technologies
- Reduction in overall business risk by incorporating new technologies and security controls

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

The workshop comprises the following Security capabilities and questions:

We assess your organisation's Network Security Capability maturity.

Security Capability	Question	Question Background
Anti-Malware	Is a network level Anti-Malware solution in-line for all traffic?	By addressing malware at the application and network level, you restrict the threat closer to the source and provide full network coverage regardless of endpoint.
Anti-Spyware	How do you control and prevent malicious command-and-control activities?	DNS sinkholing and URL filtering capabilities are an effective method for preventing C&C flows from leaving your network if a device is compromised
Sandboxing	How do you ensure non-sensitive files from all traffic on all ports are sent to an automated malware analysis solution?	Sandboxing suspect files and allowing them to be analysed is a critical security capability against unknown threats
Automated Malware Analysis	Are IOCs found in malicious files automatically turned into network and endpoint prevention updates?	Once an unknown threat has been identified, your security environment must be made aware as quickly as possible in order to contain that threat. Any delay due to manual inspection or verification increases the risk of further issues
Content Updates	How often do you perform content updates for threat prevention capabilities (AV, IPS, C2, DNS, URL)?	Continuous and timely update of known threat ensures that you are protected from modern attack vectors.

Application Control	Is application access controlled in network security policies?	Application enforcement removes the reliance on port and protocol based restriction and only allows the specific applications chosen. Defining a set of allowed applications has a number of benefits for network speed and simplicity beyond the security functions
Application Visibility	Can you identify applications in network traffic logs?	Application visibility is a key step in moving to a comprehensive policy base that prevents unusual and suspect traffic from using legitimate ports and services allowed by a port/protocol policy set.
Unidentified Traffic	How are unauthorized and unidentifiable applications identified and controlled at the network level? (e.g. evasive, tunneling, remote-access, unknown, ...)?	Once all of your known applications are defined, the remaining network traffic is identified as unknown. Typically you will either want to build custom applications to categorise this traffic, or block it as a known threat vector.
Asset Discovery	Do you maintain an active list of assets within your network? Is is automated or manual?	You cannot protect what you cannot identify. Maintaining an active list of all workstations, devices, network infrastructure is important when analysing your overall vulnerability landscape
Compliance Standards	How well do you adhere to a compliance standard? NIST, ISO27001, CIS etc	Compliance standards create a security baseline for people, process and technology to help build a robust security environment.
Email Security	How do you prevent malicious emails from reaching the end user for both corporate and personal email?	Email is one of the most common attack vectors. Education and security controls both aid in preventing attacks from malicious email
File Transfer	How is the transfer of files controlled in both download and upload direction?	When you understand the flow of files between network segments, and the applications delivering them, you can make policy decisions that enhance your overall security posture
Sensitive Data Visibility	Do you identify sensitive content in network traffic?	With sensitive data, it's important to identify as much context as possible. ie Who, What, Why, When in order for the correct decision to be made. SSL Decryption and data inspection drive this capability
Sensitive Data Control	Do you prevent sensitive content from leaving the network?	Data exfiltration can occur through legitimate paths or through compromise so it's important to be able to track the flow of data and prevent critical data from leaving the network
Decryption Coverage	What is the decryption coverage for the encrypted traffic? Is there any SSL Decryption (inbound or outbound) applied to traffic.	The majority of traffic to and from the internet is now encrypted and attackers are utilising SSL connections to bypass security layers unable to inspect
Decryption Control	How do you control traffic that can not be decrypted due to technical reasons (certificate pinning, unsupported ciphers, ...)?	

Invalid Certificates	How do you prevent encrypted traffic to websites with invalid or expired certificates?	
IOT Segmentation	How are you securing and segmenting IOT devices?	IOT devices are increasingly used as a threat vector so being able to identify and protect these devices reduces the risk of vulnerability
Out of Band Management	How do you restrict access to network infrastructure management?	
DNS Restrictions	Do you restrict outbound DNS and DNS forwarders to an approved list?	
DNS Tunneling	How do you inspect DNS traffic for tunneling activity?	
DNS DGAs	Are you able to detect and block malicious domains created by domain generation algorithms? (DGAs)	Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers.
DNS Sinkhole	Do you sinkhole suspicious DNS queries to validate the internal source IP?	Without sinkhole, an internal DNS server will typically display as the source address in threat logs making it difficult to identify an infected device.
DoS	How do you mitigate DOS attacks?	Denial of Service attacks are usually external, but can also be launched within the network so it's important to ensure coverage around critical assets or vulnerable segments of the network
Reconnaissance	How do you mitigate and stop internal and external Recon activities?	Port scanning and other recon activities may not be malicious by themselves but often lead to a breach as a result. Preventing Recon from occurring helps prevent further exposure
Centralised Logging	Are logs forwarded to a central logging repository for security monitoring purposes?	Audit logging should be consistent and centralised across cloud platforms to provide an efficient and comprehensive audit trail when required
Log Retention	What is your log retention period for proactive monitoring and behavioral analysis purposes?	
Log Storage	Do you backup logs to internal/external storage to meet compliance requirements around long-term log retention?	

Segmentation	How do you segment your network environment up to layer 7 to prevent lateral threat movement?	Understanding the layer 4 network topology helps to ensure logical segments exist and identify security controls between segments. True layer 7 enforcement means being able to identify traffic by applications and/or user and having the ability to restrict or allow traffic flow based on those parameters
Micro Segmentation	Have you implemented microsegmentation in any network segments?	
Multi-Factor Authentication	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
User Visibility	How do you track user activity at the network level?	Monitoring user access to resources is the first step to identifying normal and abnormal behaviours. In some areas of the network, user enforcement may not be necessary however for forensic purposes, having the ability to show user activity is vital to understanding the chain of events
User Control	Is access to systems based on user identity controlled by a firewall or other network device?	While most applications have some form of user control, network level user access control creates a consistent environment and removes the complexity of managing multiple user authentication sources
Behavioral Analytics	Are you looking for abnormal activities of machines and users who are accessing company digital assets?	With proper context, analysing network traffic can identify "low and slow" threats that may evade other means of detection. In addition, it can be used to locate and prevent insider threat vectors
Vulnerability Discovery	Do you conduct regular pentesting of your environment?	
Vulnerability Management	Is a network-level Vulnerability protection solution in line for all traffic?	In addition to host based vulnerability protection, network VP provides a safeguard for IOT devices, and other network connected assets that do not have endpoint coverage
Vulnerability Remediation	Do you have a process to remediate vulnerabilities in infrastructure as they occur?	
Dynamic Block Lists	How do you automatically block known malicious IP Addresses and URLs, based on threat intelligence from third-party feeds?	IP and DNS hostname dynamic lists can be sourced from multiple external locations and applying them in firewall policy allows for near real time protection against known threats

Credential Theft Prevention	How do you prevent Credential Phishing attempts?	Corporate credentials are often the weakest link in the security portfolio so it's important to know where they are being used outside of the organisation. In addition, some phishing campaigns are incredibly complex so have an automated system to alert on and restrict credential use is important
URL Filtering	Do you block known bad URLs across all ports, or use a Proxy for HTTP and HTTPS traffic only?	URL filtering limits access by comparing web traffic against a database to prevent employees from accessing unproductive, harmful sites such as phishing pages.
URL Logging	Do you alert, log and correlate on known-bad, unknown and IP-based URLs?	If a URL has no matching category or is an IP rather than DNS name, it can be missed in URL logs or allowed through so it's important to validate these reports and ensure that this risk is understood if it exists