TITANIA

PCI DSS 4.0

Viewing and managing compliance through an attacker's lens

Understand your exposure to real-world threats

Ensuring that network infrastructure complies with PCI DSS 4.0 is a proven way to strengthen the security of an organization's Cardholder Data Environment (CDE). Whilst prioritizing non-compliances for effective remediating action not only improves compliance posture, it significantly reduces network risk.

It's why Nipper's new PCI DSS 4.0 report has been developed to provide a fast, accurate and efficient way to prioritize identified device vulnerabilities by their risk to compliance. Run at scale across large or multiple CDEs, with a Nipper OmniSight deployment, this report will provide a complete view of compliance risks. However, it may highlight more vulnerabilities than it is possible to mitigate between audits, particularly when Nipper OmniSight's proactive assessment capabilities have been enabled. So knowing which risks are most exploitable can be transformative for organizations that are looking to target resources and fast-track remediation to protect their attack surface. This requires a further layer of analysis.

Risk-prioritized remediation

Historical vulnerability data dating back to 2019 reveals that only 4% of known vulnerabilities have been used by attackers in the wild, and according to CISA, it is known exploited vulnerabilities (KEVs) that should be the top priority for immediate remediation.

KEV data also needs to be overlaid with information about how adversaries operate, if risk owners are to truly understand their CDE's exposure to real-world attacks. By examining the tactics, techniques and procedures (TTPs) that are being used by threat actors and threat groups to target similar organizations, network owners can start to examine their risk posture, asking questions such as:

- What are we doing to prevent 'privilege escalation'?
- What is our current risk posture to this technique that was recently used to exploit our competitor?
- How susceptible are we to particular types of ransomware attack?

Knowledge bases from the likes of MITRE provide a wealth of threat intelligence that helps organizations keep track of TTPs. And using MITRE ATT&CK posture data to augment misconfiguration, non-compliance and vulnerability data creates a very powerful dataset to feed into risk prioritization and remediation plans.

Zero-in on exploitable vulnerabilities

To stay on top of software vulnerabilities requires regular patching of devices. But it is not possible to patch to remediate a weak admin password or an insecure routing protocol. These types of misconfiguration vulnerabilities remain on the device, posing a risk to the network, until they are found and fixed.

Which is why Nipper OmniSight provides MITRE ATT&CK posture from two different vantage points across networking devices: device OS software vulnerabilities and device configurations.

Nipper OmniSight then helps prioritize and expedite remediation with device-specific guidance on how to mitigate the risks, and can proactively re-assess changes to confirm that hardening activities have been successful.

Used to manage 'configuration as code' Nipper OmniSight can also test pre-production changes, aid recovery from operational incidents, and perform root cause analysis of changes that caused the incident.

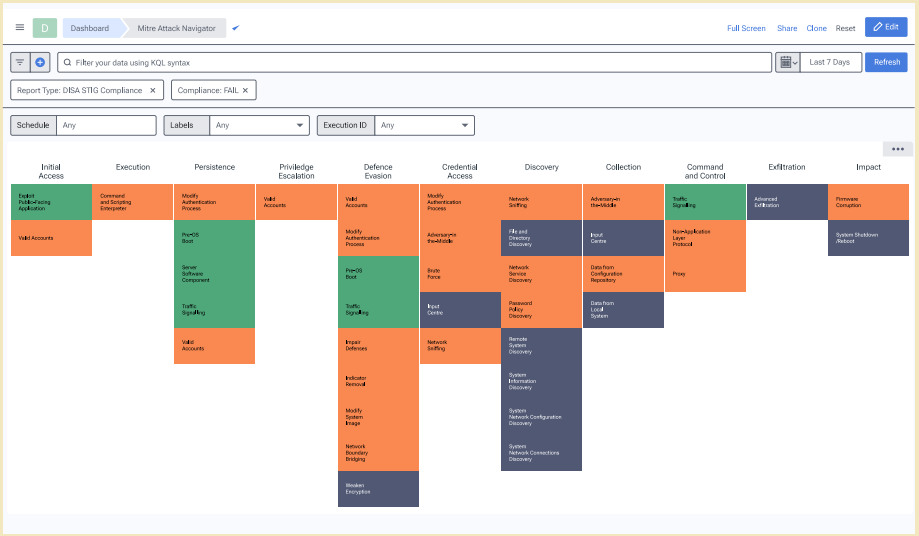
Nipper OmniSight: A game changer

Delivering a game-changing way to view these network risks from an attacker's perspective, the MITRE ATT&CK dashboard in Nipper OmniSight shows how the network would most likely be targeted by threat actors, operating right now.

Automatically overlaying MITRE ATT&CK exposure analysis onto PCI DSS 4.0 non-compliance analysis* helps to determine whether the CDE is also vulnerable to adversarial tactics and techniques being used in the real-world. And prioritizing remediation workflows according to these insights will harden the CDE against the most likely attacks.

Nipper OmniSight can achieve this level of insight, automatically, and can be integrated with remediation tech stacks to further reduce the mean time to remediate vulnerabilities that are exposing the network.

* STIG, CCI, NIST 800-53, NIST 800-171 and CMMC risk lenses can also be overlaid with MITRE ATT&CK posture analysis for next-level network exposure management.



Equipping threat-hunting teams

Nipper OmniSight reporting can also help with forensic analysis, to determine exposure following an attack. Understanding where an attack could have proliferated based on network segmentation and device vulnerability at the time of the first indicator of compromise, helps determine how wide to cast the net in terms of threat hunting. So Nipper OmniSight's historic MITRE ATT&CK posture data can guide threat hunting teams to inform incident response.

Arrange a demo to see for yourself how Nipper OmniSight's MITRE ATT&CK posture analysis can be used to shut down attacks, forensically examine the extent of compromise, and defend against future breach.

titania.com/try/demo

Why Titania

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally.

Whether organizations need real-time visibility and analysis of every network change to get ahead of threats, segmentation violations, and potential network disruptions. Or scheduled network posture and device vulnerability assessments to enhance attack surface security and demonstrate compliance. We have a solution for every stage of the journey to network readiness and resilience.

USA
Suite 6500, 2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England, W1W 5PF

TITANIA

titania.com