PCI Security Standards Council

Continuously Viewing and Managing PCI DSS Compliance Through an Attacker's Lens

Ian Robinson, Chief Architect, Titania Ltd

TITANIA

Continuous Compliance

How can you make the shift from ad-hoc sampled assessments to assessing every device in your CDE for continuous compliance?

Avoiding sampling where automation allows	Regularly assess network infrastructure	Assure the CDE remains adequately segmented

NIPPER ENTERPRISE

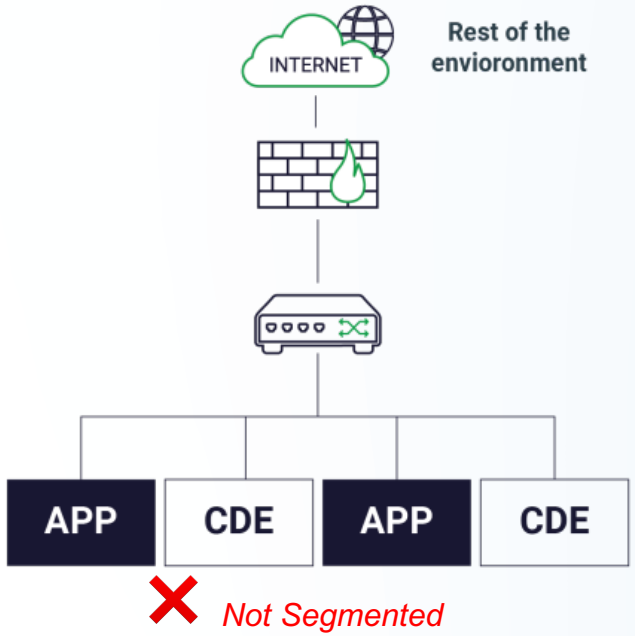
1. How to assure that networks are adequately segmented to minimize the attack surface
2. How to generate evidence-based reports of pass/fail compliance with PCI DSS 4.0
3. How to prioritize and expedite mean time to fix non-compliances to shut down real-world threats

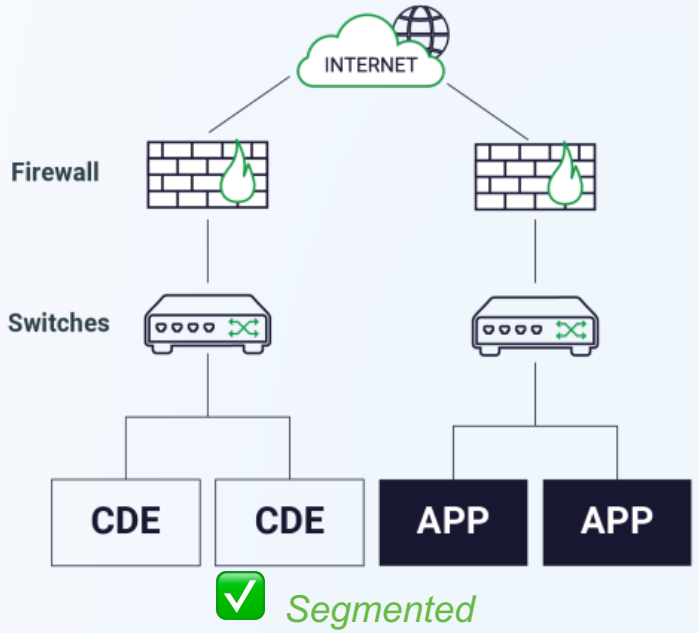
PCI Security Standards Council

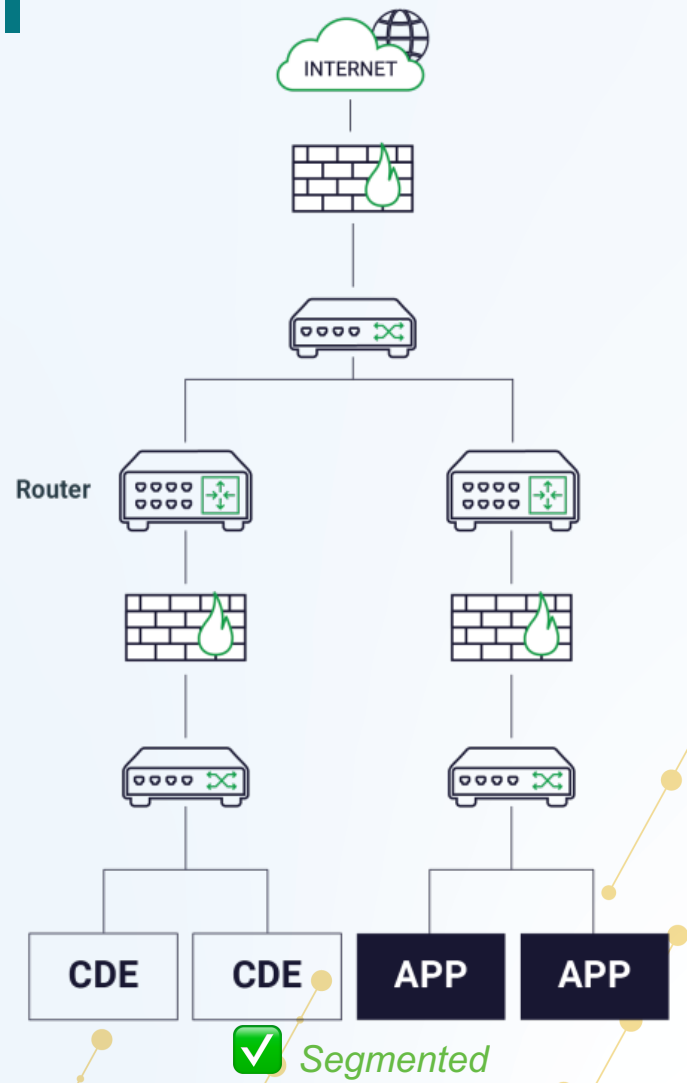
The Ultimate Mitigating Control

Secure and PCI DSS 4.0 compliant network infrastructure

Effective network segmentation relies on the security and compliance of every router, switch and firewall in the Cardholder Data Environment...







PCI Security Standards Council

Reducing Attack Surface with Effective Segmentation

"Zero-Trust Segmentation (ZTS) isolates critical resources so that if a network is compromised, the attacker can't gain access."

FORRESTER

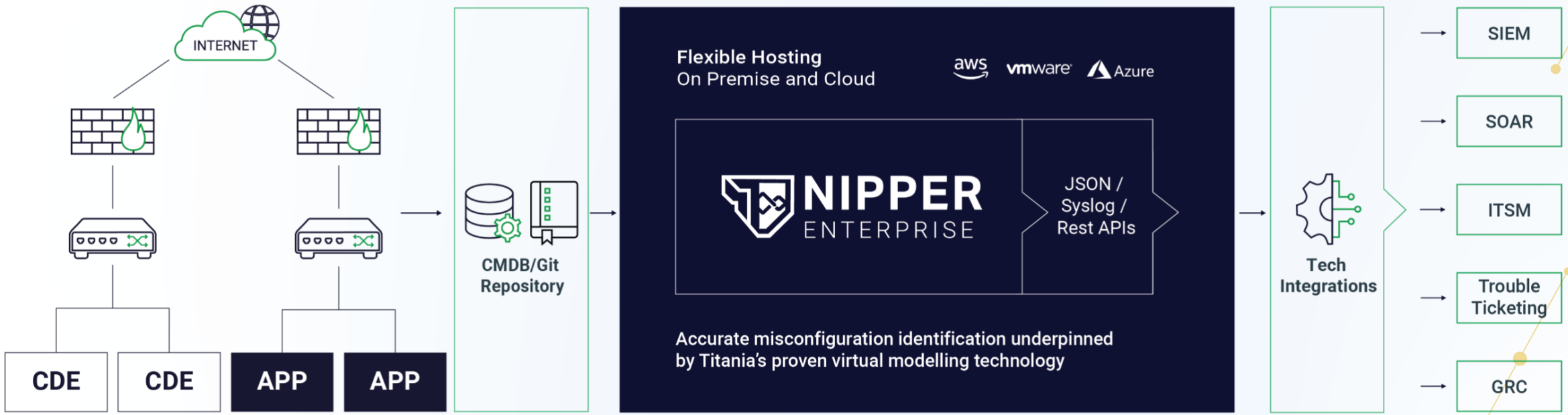
"Organizations that have adopted ZTS save an average of $20.1m in application downtime and deflect five cyber disasters per year."

VentureBeat

PCI Security Standards Council

Effective Network Segmentation – at scale

How does Nipper Enterprise leverage your network segmentation?



?? *Segmented* ??

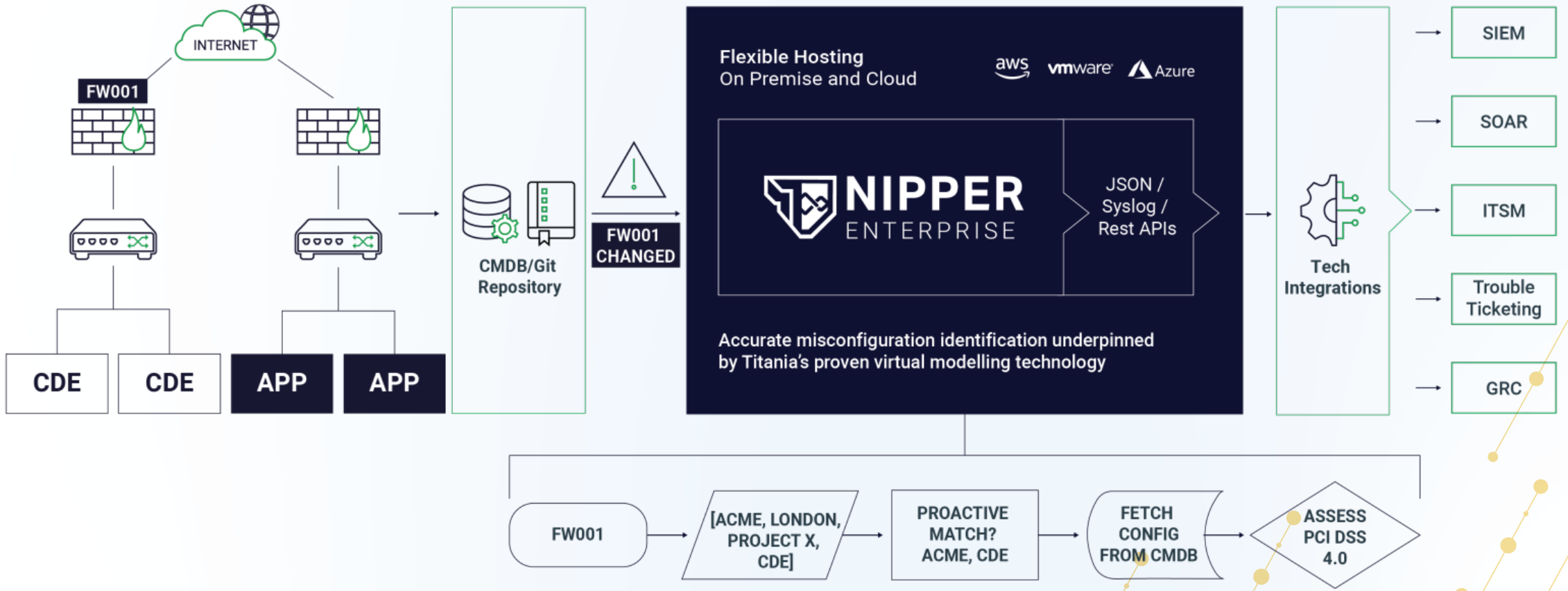
It was segmented yesterday, but does it remain so today?

1. *Syncs with CMDB and inherits segmentation data >*
2. *Schedules & manages PCI DSS Compliance assessments >*
3. *Evidences compliance >*
4. *Prioritizes remediation of non-compliances >*

PCI Security Standards Council

Proactive Assessment – at scale

How does Nipper Enterprise allow you to assess only what's changed?



PCI Security Standards Council

Beyond Segmentation

How to prioritize remediation by viewing and managing risk through an attacker's lens

*"Vulnerability management (VM) has long been viewed as a compliance function **instead of a threat-prevention capability**…. Look to augment your VA tool …. with breach and attack simulation (BAS) and attack surface management (ASM) tools"*

Gartner®

"For over 10 years only between 7.6% and 12.6% of all (software) vulnerabilities have been exploited…. Organizations should focus on active threats instead of addressing thousands of vulnerabilities that may never occur in real-world attacks."

CISA CYBER+INFRASTRUCTURE

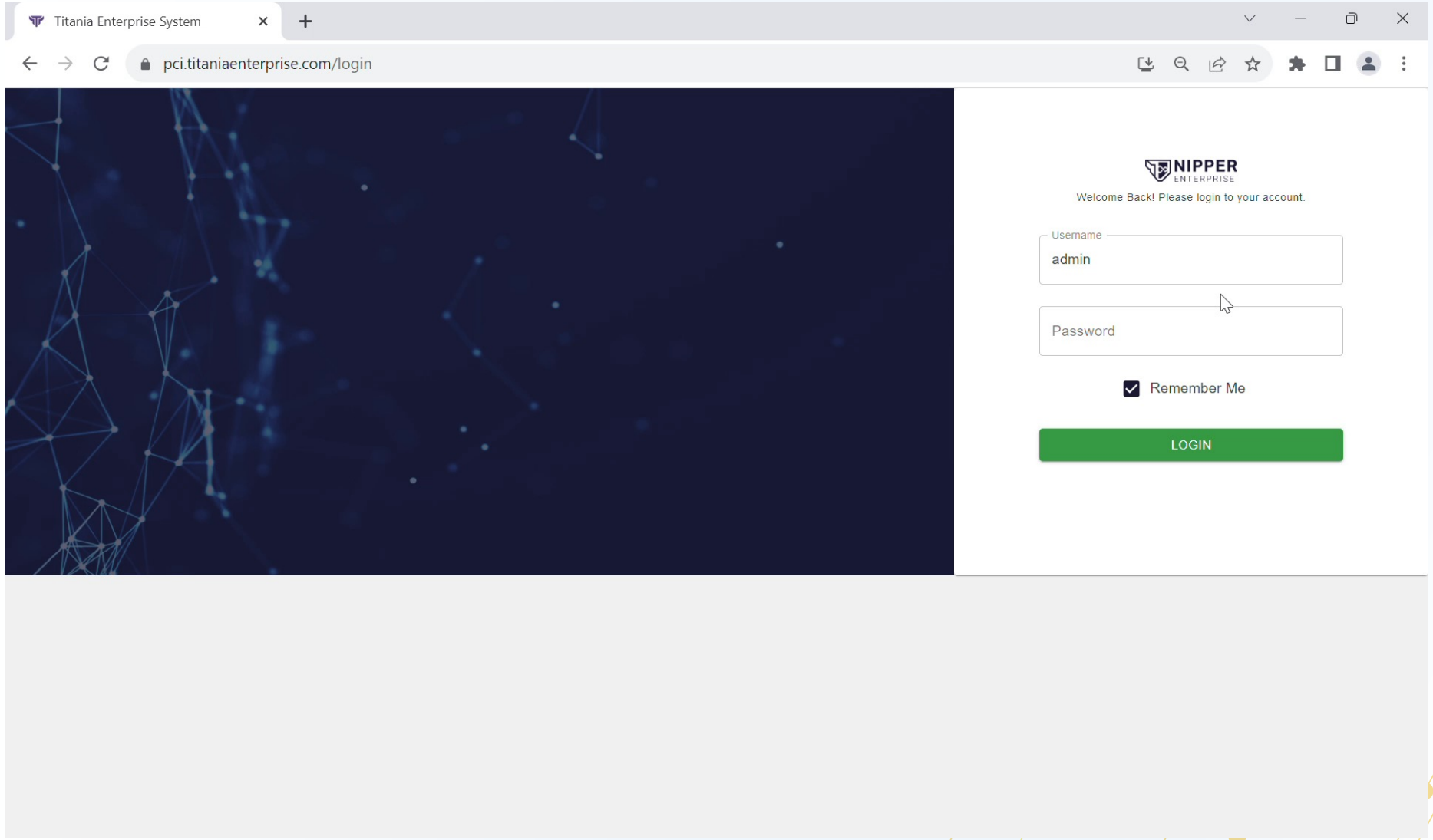
CAPEC™ Common Attack Patterns https://capec.mitre.org/

MITRE | ATT&CK® Tactics & Techniques https://attack.mitre.org/

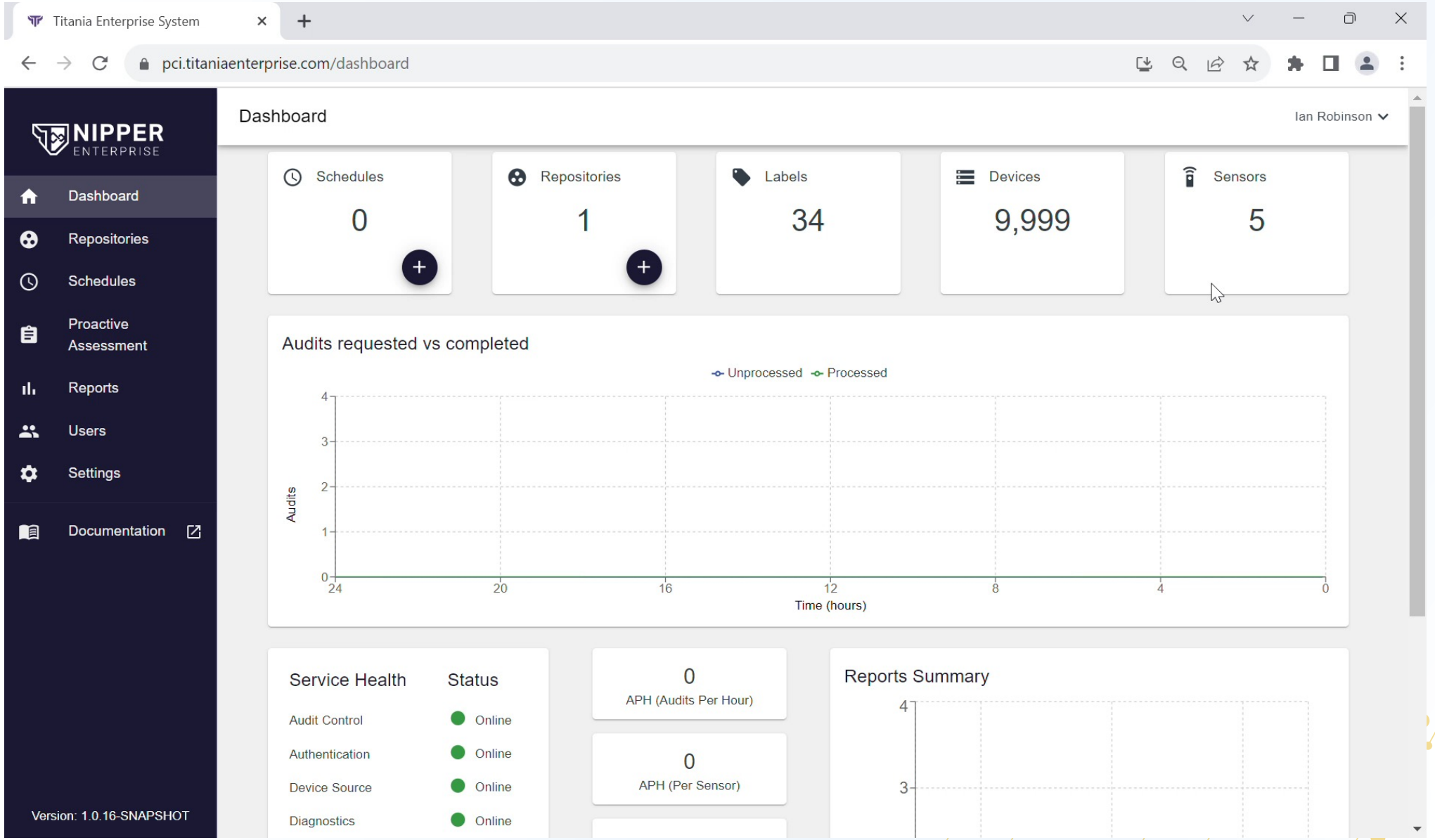
PCI Security Standards Council

Nipper Enterprise

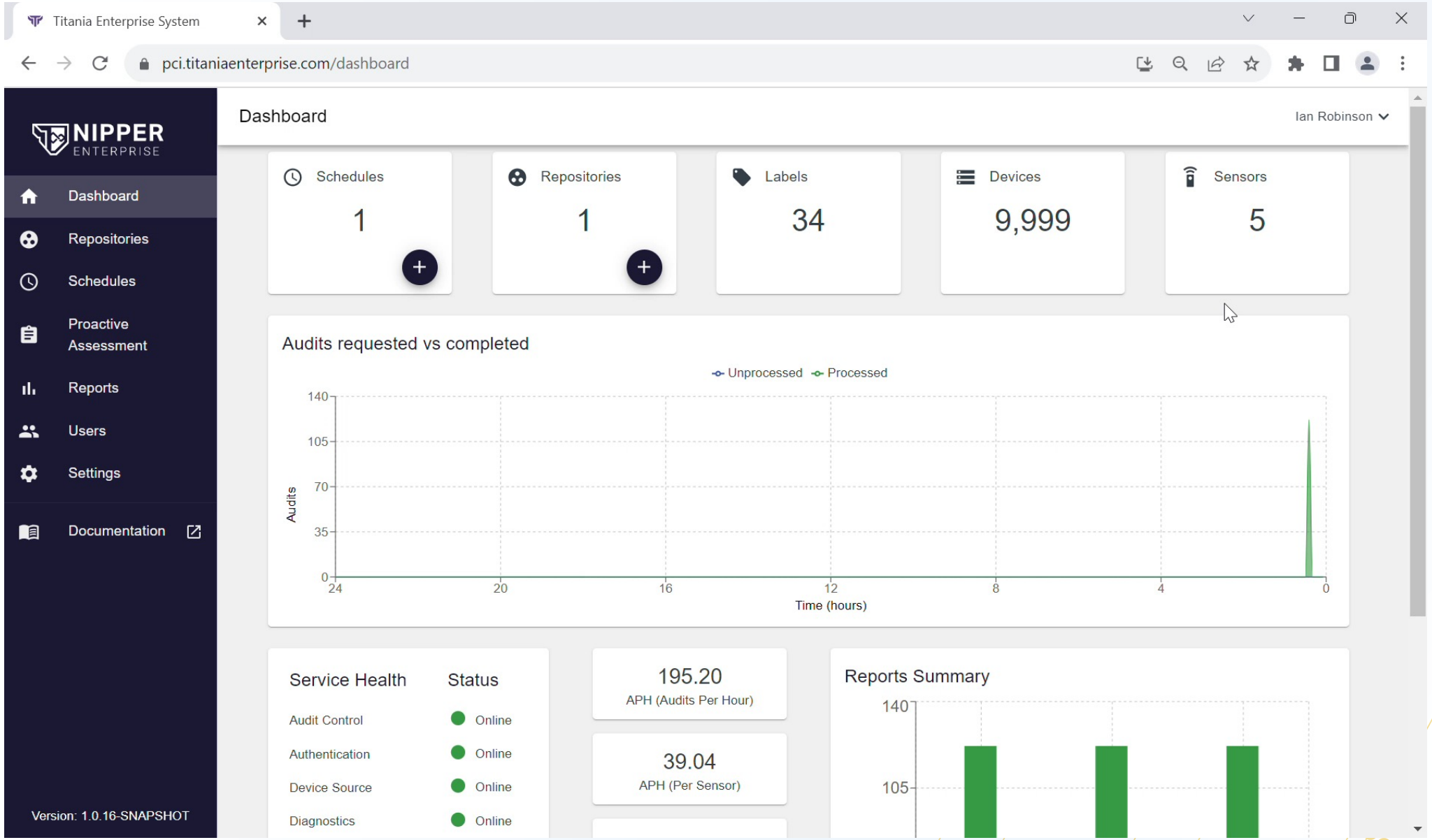
Continuous ZT Network Segmentation assurance, PCI DSS v4.0 compliance assurance and Attack Surface Management assurance – at scale



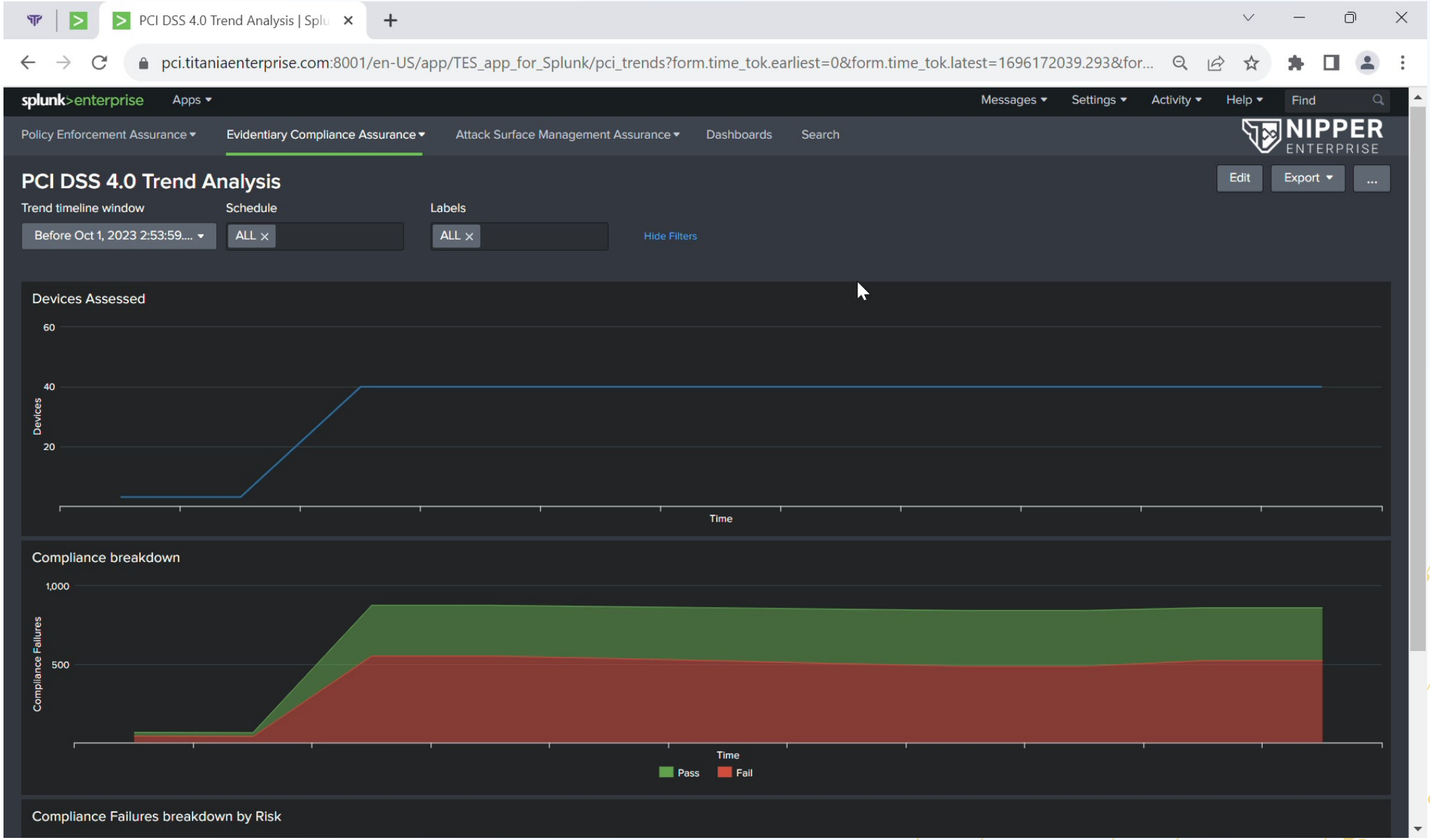
Nipper Enterprise – Scheduling assessments



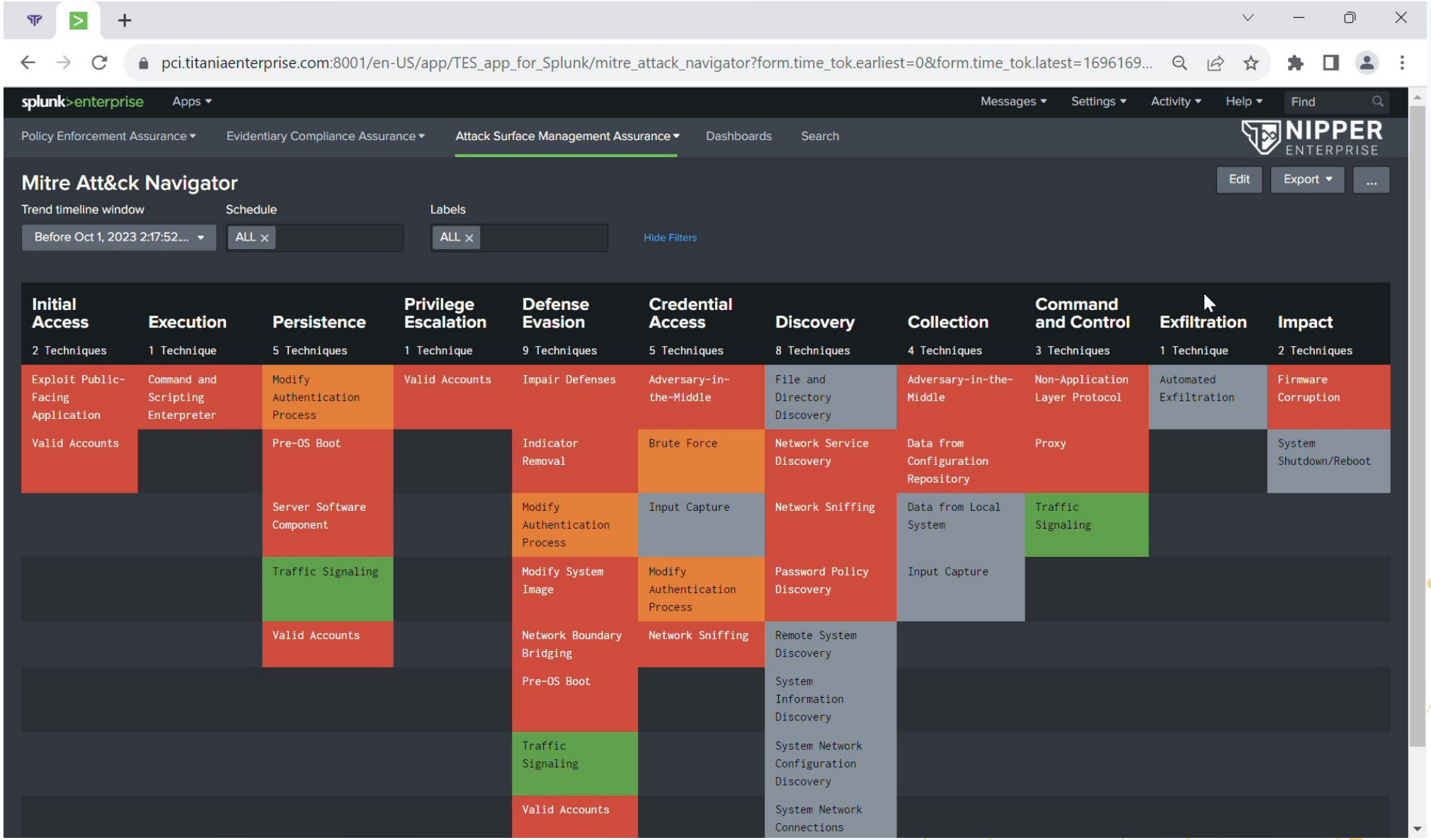
Nipper Enterprise – Evidence based Compliance reporting



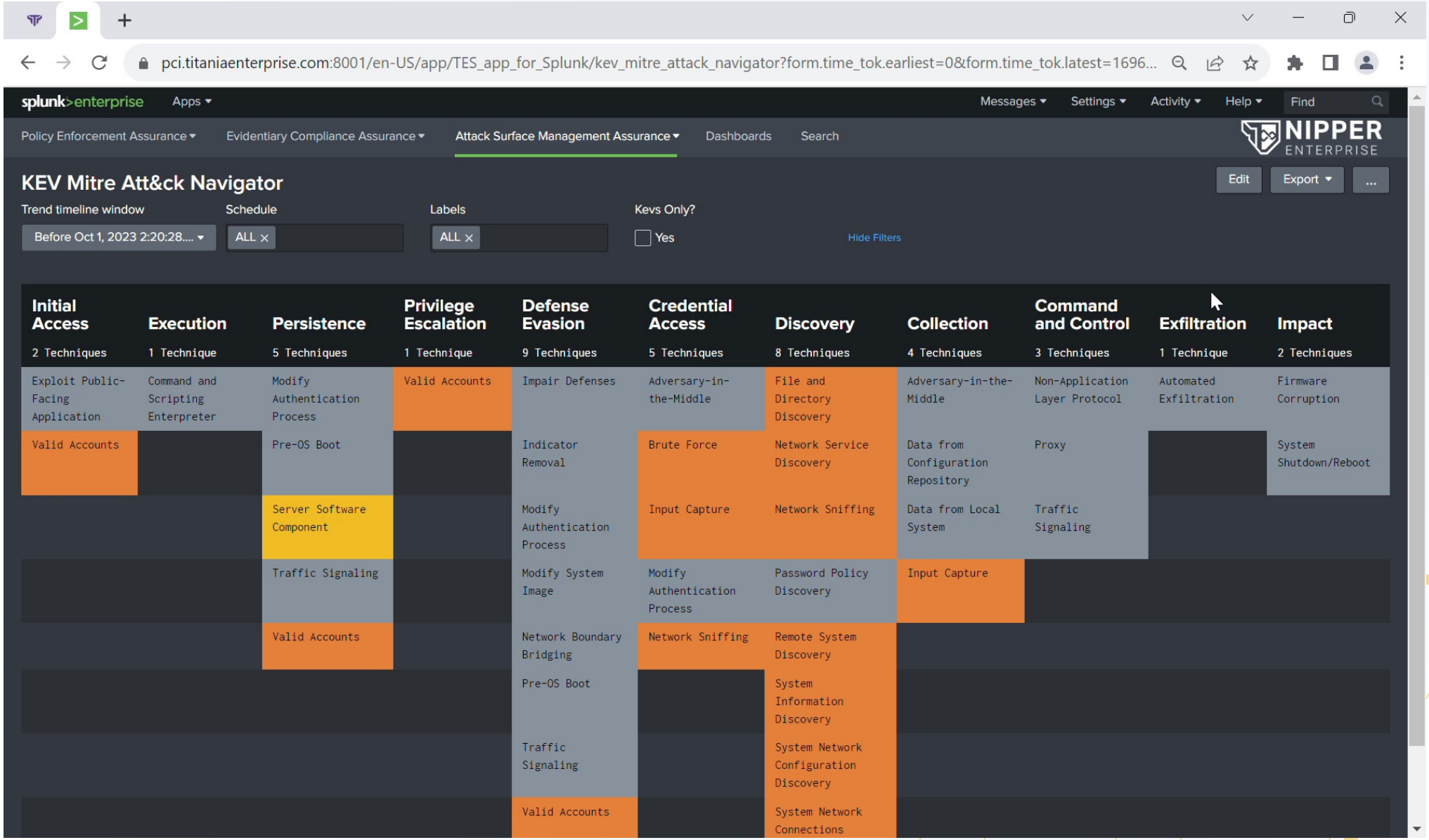
Nipper Enterprise – PCI DSS v4.0 Compliance Assurance



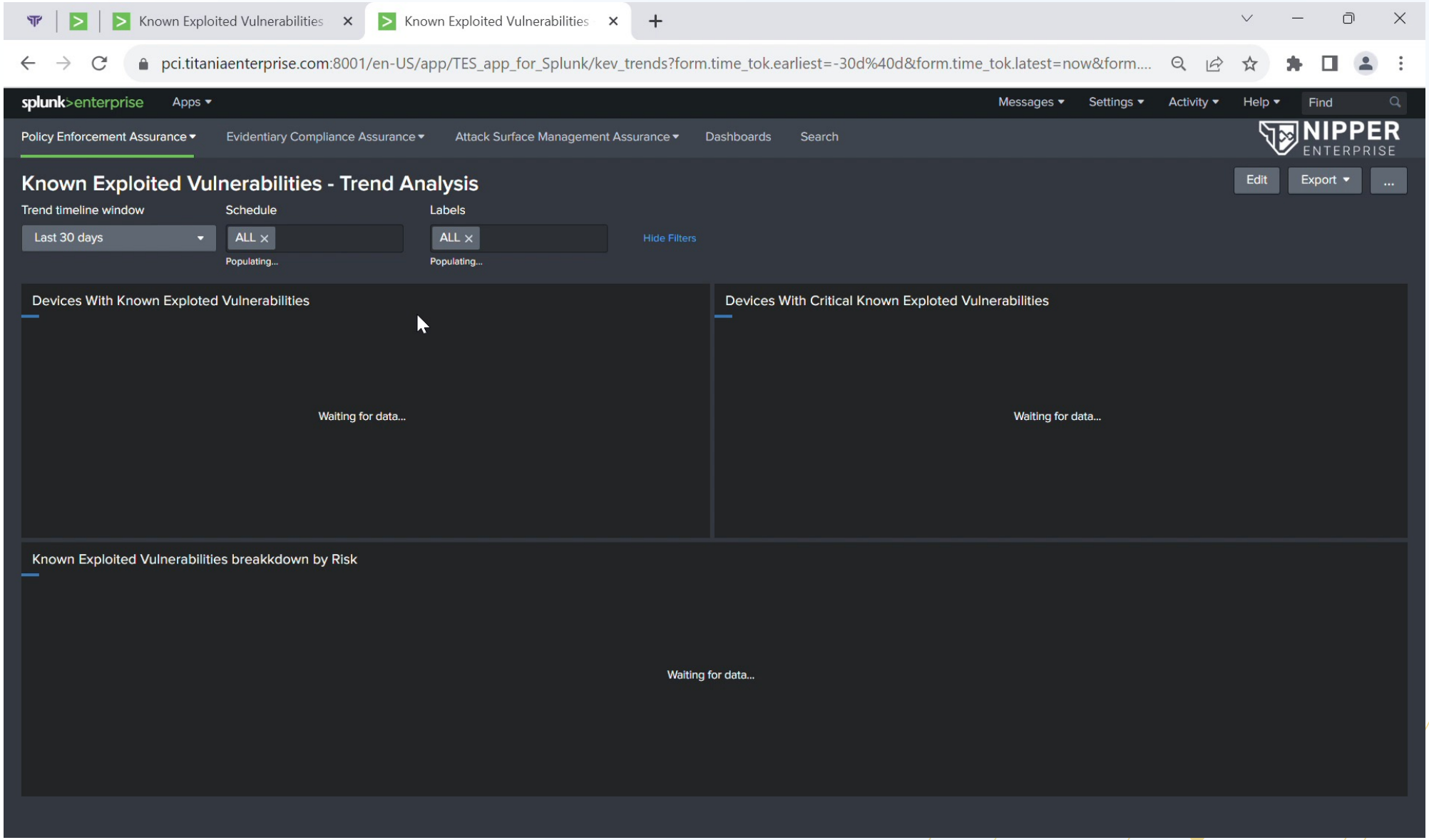
Nipper Enterprise – ASM Assurance (Configuration)



Nipper Enterprise – ASM Assurance (CVE Software Vulnerabilities)



Nipper Enterprise – ASM Assurance (CISA Known Exploited Vulnerabilities)



Thank you

If you have any questions...

Stand #4

- **Request a tailored demo**
- **Proof of Value assessment**

ian.robinson@titania.com

https://www.linkedin.com/in/ian-robinson-92ab85276/

PCI Security Standards Council

Europe Community Meeting 2023

PCI Security Standards Council