



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

Ian Robinson, Chief Architect, Titania Ltd



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

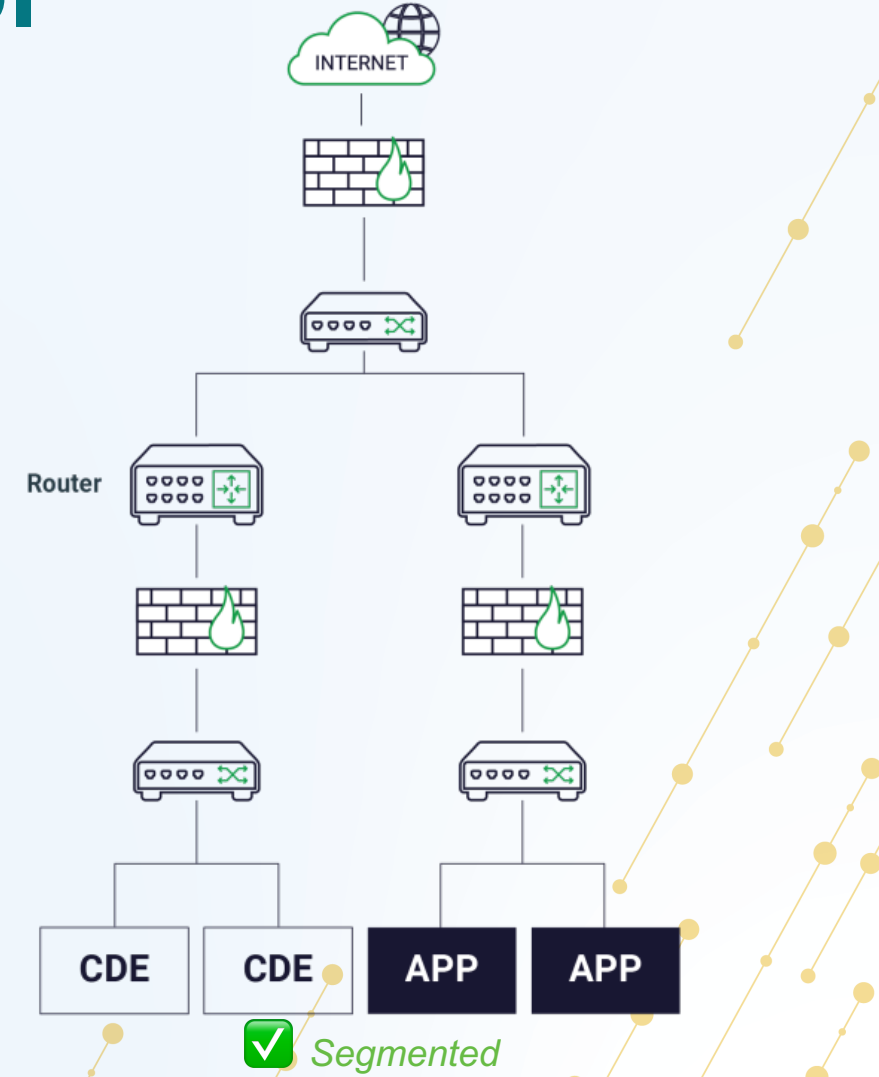
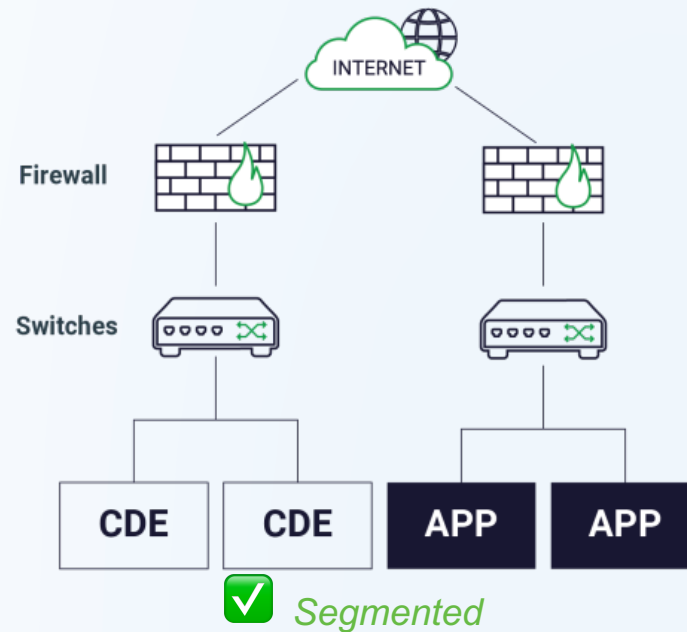
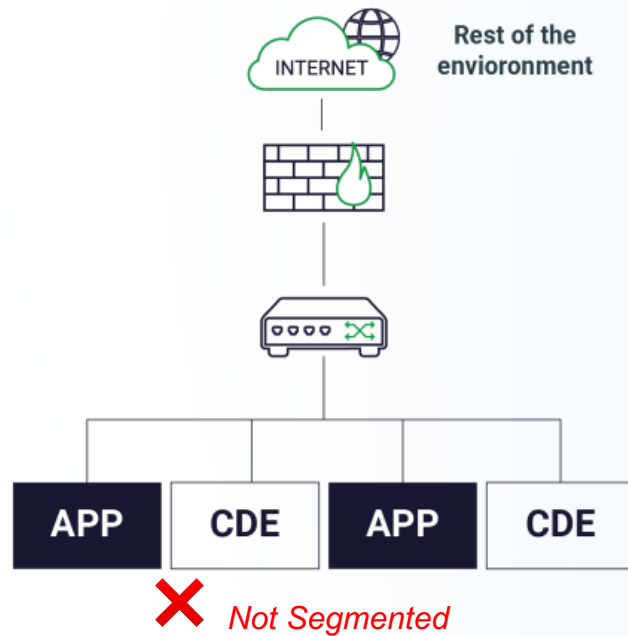


1. How to assure that networks are adequately segmented to minimize the attack surface
2. How to generate evidence-based reports of pass/fail compliance with PCI DSS 4.0
3. How to prioritize and expedite mean time to fix non-compliances to shut down real-world threats

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...



Reducing Attack Surface with Effective Segmentation

--- ATTACK SURFACE MANAGEMENT ---

ASSET
DISCOVERY

ASSET
VALIDATION

ASSET
INVENTORY

ASSET
ASSESSMENT

servicenow

 **NIPPER**
ENTERPRISE

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

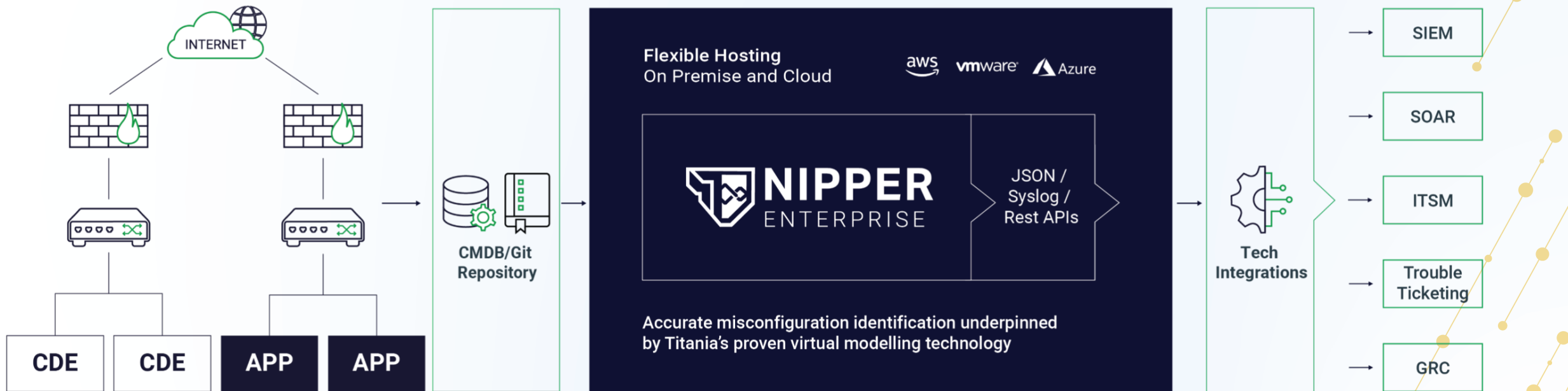
FORRESTER

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

VentureBeat

Effective Network Segmentation – at scale

How does Nipper Enterprise leverage your network segmentation?



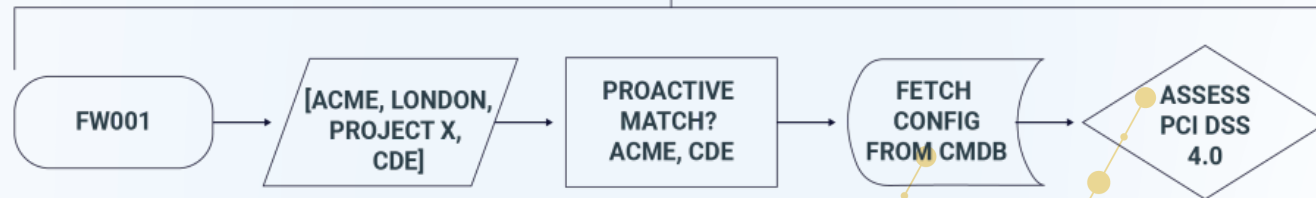
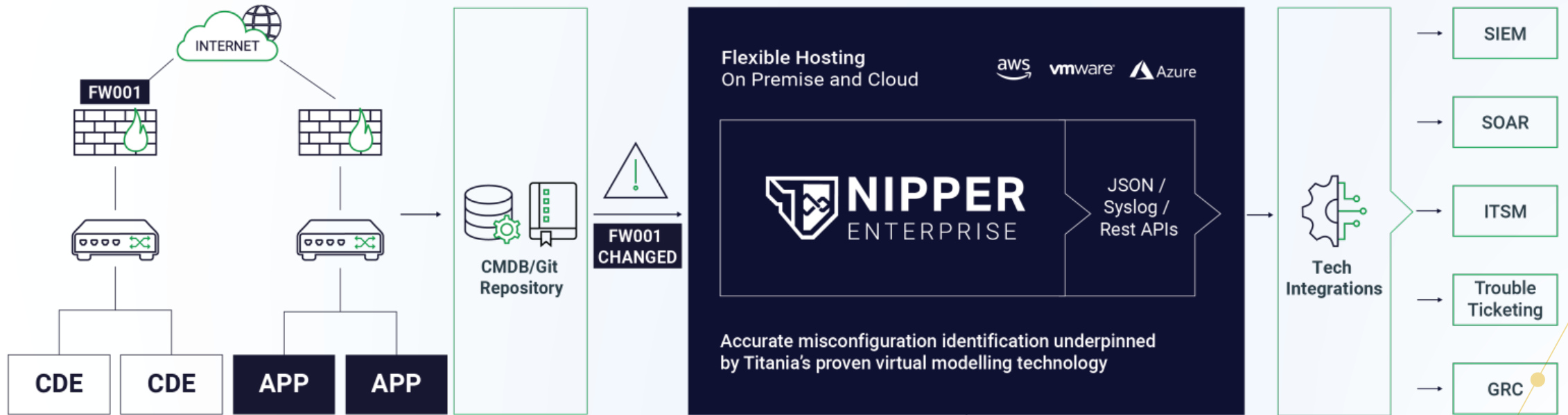
?? Segmented ??

*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 >

Proactive Assessment – at scale

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



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.”



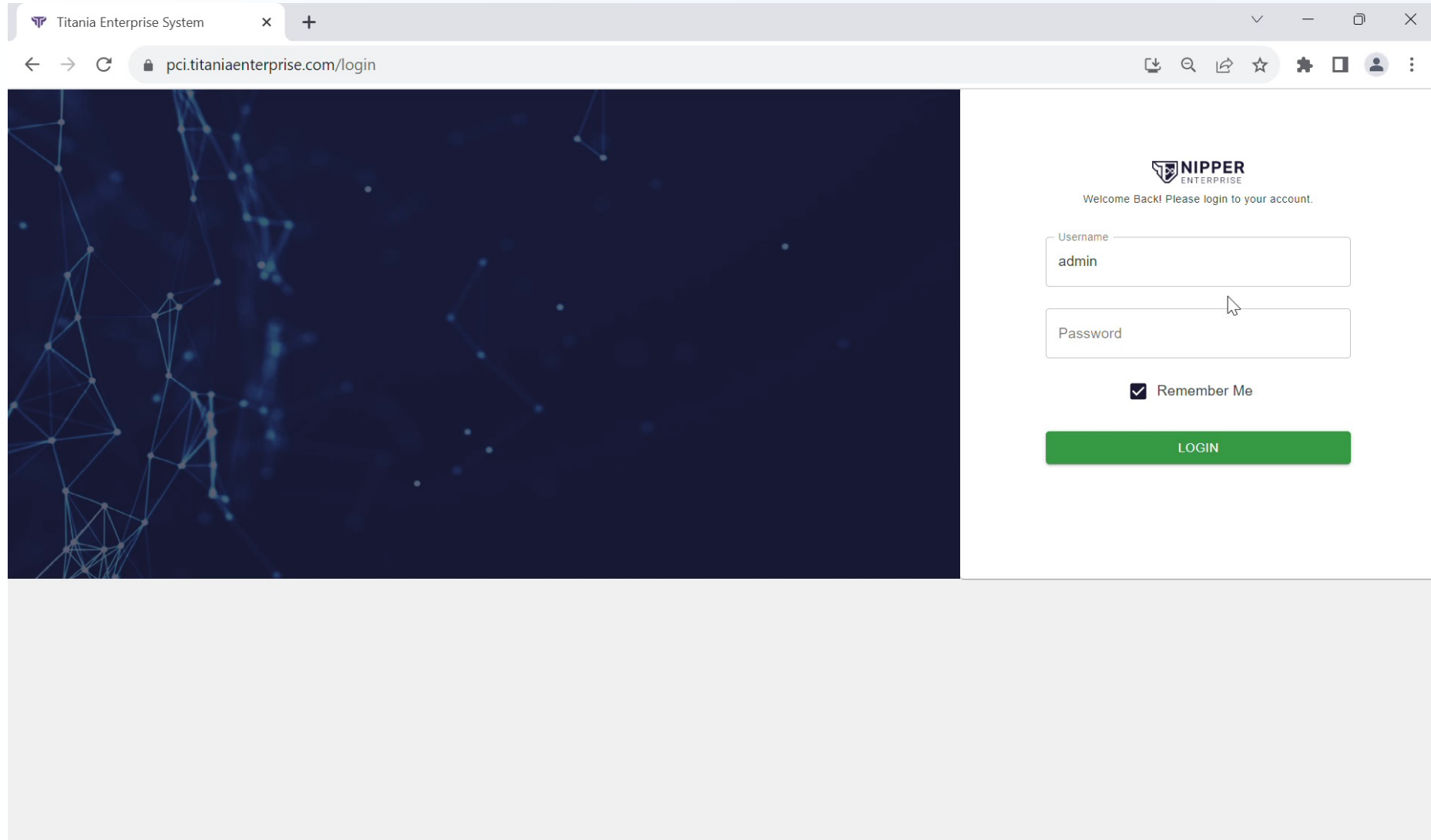
Common Attack Patterns
<https://capec.mitre.org/>

MITRE | ATT&CK[®]

Tactics & Techniques
<https://attack.mitre.org/>

Nipper Enterprise

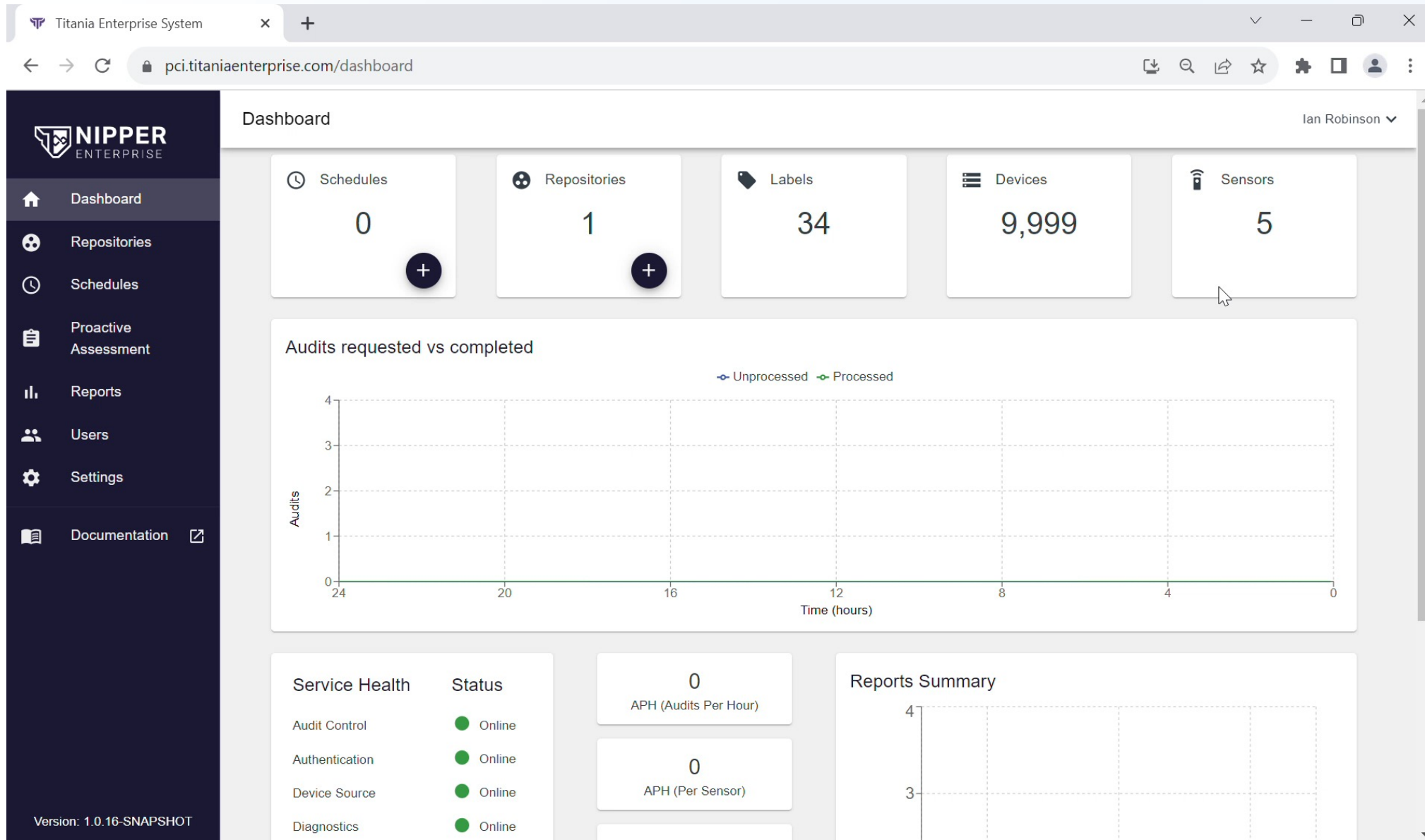
Continuous ZT Network Segmentation assurance, PCI DSS v4.0 compliance assurance and Attack Surface Management assurance – at scale



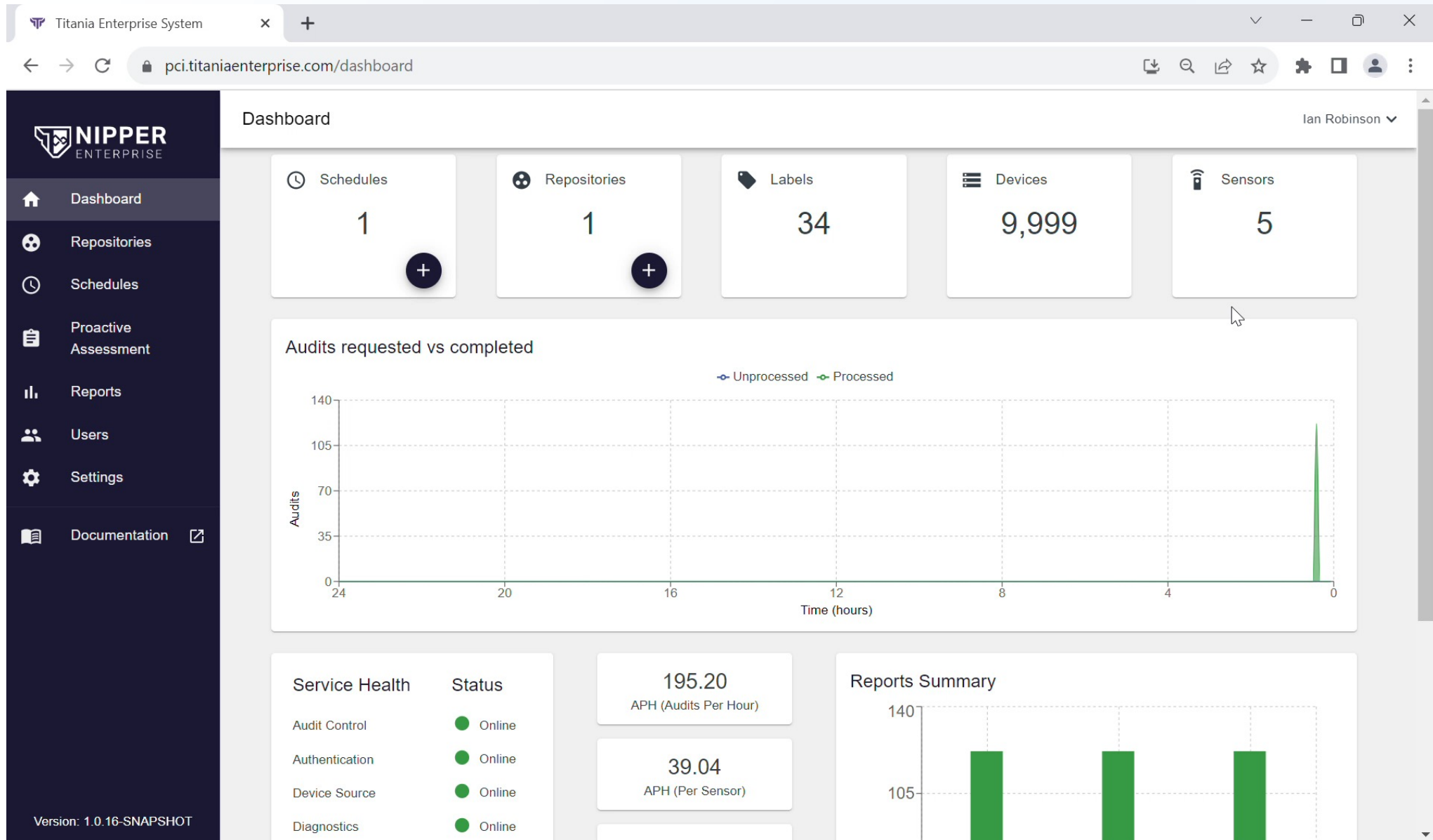
The image shows a browser window with the following details:

- Tab: Titania Enterprise System
- Address bar: pci.titaniaenterprise.com/login
- Page Content:
 - Logo: NIPPER ENTERPRISE
 - Message: Welcome Back! Please login to your account.
 - Username field: Contains "admin"
 - Password field: Empty
 - Remember Me: Remember Me
 - Login Button: A green button labeled "LOGIN"

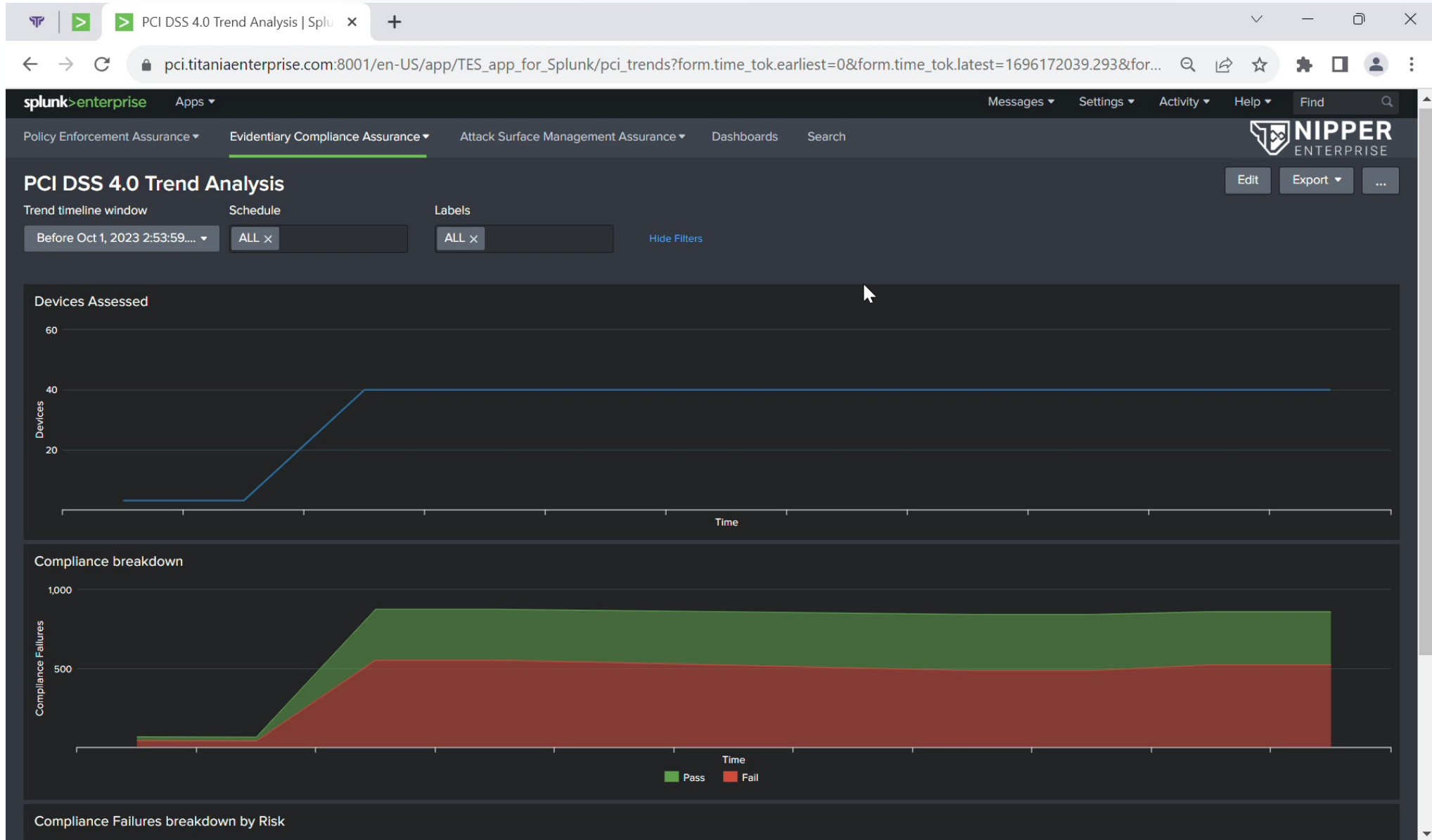
Nipper Enterprise – Scheduling assessments



Nipper Enterprise – Evidence based Compliance reporting



Nipper Enterprise – PCI DSS v4.0 Compliance Assurance



Nipper Enterprise – ASM Assurance (Configuration)

pci.titaniaenterprise.com:8001/en-US/app/TES_app_for_Splunk/mitre_attack_navigator?form.time_tok.earliest=0&form.time_tok.latest=1696169...

splunk>enterprise Apps Messages Settings Activity Help Find

Policy Enforcement Assurance Evidentiary Compliance Assurance **Attack Surface Management Assurance** Dashboards Search

NIPPER ENTERPRISE Edit Export ...

Mitre Att&ck Navigator

Trend timeline window Schedule Labels

Before Oct 1, 2023 2:17:52... ALL x ALL x Hide Filters

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration	Impact
2 Techniques Exploit Public-Facing Application Valid Accounts	1 Technique Command and Scripting Interpreter	5 Techniques Modify Authentication Process Pre-OS Boot Server Software Component Traffic Signaling Valid Accounts	1 Technique Valid Accounts	9 Techniques Impair Defenses Indicator Removal Modify Authentication Process Modify System Image Network Boundary Bridging Pre-OS Boot Traffic Signaling Valid Accounts	5 Techniques Adversary-in-the-Middle Brute Force Input Capture Modify Authentication Process Network Sniffing	8 Techniques File and Directory Discovery Network Service Discovery Network Sniffing Password Policy Discovery Remote System Discovery System Information Discovery System Network Configuration Discovery System Network Connections	4 Techniques Adversary-in-the-Middle Data from Configuration Repository Data from Local System Input Capture	3 Techniques Non-Application Layer Protocol Proxy Traffic Signaling	1 Technique Automated Exfiltration	2 Techniques Firmware Corruption System Shutdown/Reboot

Nipper Enterprise – ASM Assurance (CVE Software Vulnerabilities)

splunk>enterprise Apps

Policy Enforcement Assurance Evidentiary Compliance Assurance **Attack Surface Management Assurance** Dashboards Search

KEV Mitre Att&ck Navigator Edit Export ...

Trend timeline window Schedule Labels Keys Only? Yes Hide Filters

Before Oct 1, 2023 2:20:28... ALL x ALL x

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration	Impact
2 Techniques Exploit Public-Facing Application	1 Technique Command and Scripting Interpreter	5 Techniques Modify Authentication Process	1 Technique Valid Accounts	9 Techniques Impair Defenses	5 Techniques Adversary-in-the-Middle	8 Techniques File and Directory Discovery	4 Techniques Adversary-in-the-Middle	3 Techniques Non-Application Layer Protocol	1 Technique Automated Exfiltration	2 Techniques Firmware Corruption
Valid Accounts		Pre-OS Boot		Indicator Removal	Brute Force	Network Service Discovery	Data from Configuration Repository	Proxy		System Shutdown/Reboot
		Server Software Component		Modify Authentication Process	Input Capture	Network Sniffing	Data from Local System	Traffic Signaling		
		Traffic Signaling		Modify System Image	Modify Authentication Process	Password Policy Discovery	Input Capture			
		Valid Accounts		Network Boundary Bridging	Network Sniffing	Remote System Discovery				
				Pre-OS Boot		System Information Discovery				
				Traffic Signaling		System Network Configuration Discovery				
				Valid Accounts		System Network Connections				

Nipper Enterprise – ASM Assurance (CISA Known Exploited Vulnerabilities)

The screenshot displays the Nipper Enterprise web interface. The browser address bar shows the URL: `pci.titaniaenterprise.com:8001/en-US/app/TEs_app_for_Splunk/kev_trends?form.time_tok.earliest=-30d%40d&form.time_tok.latest=now&form...`. The application header includes the Splunk logo and navigation options like 'Policy Enforcement Assurance', 'Evidentiary Compliance Assurance', and 'Attack Surface Management Assurance'. The main dashboard title is 'Known Exploited Vulnerabilities - Trend Analysis'. Below the title, there are filter controls: 'Trend timeline window' set to 'Last 30 days', 'Schedule' set to 'ALL', and 'Labels' set to 'ALL'. A 'Hide Filters' link is also present. The dashboard contains three panels, each with the text 'Waiting for data...':

- 'Devices With Known Exploited Vulnerabilities'
- 'Devices With Critical Known Exploited Vulnerabilities'
- 'Known Exploited Vulnerabilities breakdown by Risk'

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/>



Europe Community Meeting 2023

