EINPRESSWIRE

Titania Nipper Release Simplifies Federal Agencies’ Ability to Prioritize and Remediate NIST SP 800-53 Non-Compliances

Titania’s software solution equips agencies with a critical capability lacking in more than 80 percent of federal government organizations

ARLINGTON, VA, USA, September 26, 2023 /EINPresswire.com/ -- Titania, specialists in continuous network security and compliance assurance solutions, have launched a brand new reporting capability, designed to make it quicker and easier for federal organizations to determine their NIST SP 800-53 security posture for their entire network infrastructure. The new capability can also accelerate time to remediate non-compliances with risk-prioritized remediation advice.

> “Titania’s new software capability will enable organizations to analyze their entire network infrastructure estate, accurately prioritize non-compliances, and take remediation action based on risk.”
>
> *Dean Webb, cybersecurity engineer at Merlin Cyber, a partner of Titania*

This launch comes at a time when regulators are recommending a zero-trust approach to network segmentation, where all network devices (routers, switches and firewalls) are continuously validated for compliance with policies and control frameworks like DISA STIGs and NIST SP 800-53. “The Federal Government has broadly relied on perimeter defenses which makes them soft targets for bad actors to exploit their configuration drift vulnerabilities,” stated Dean Webb, cybersecurity engineer at Merlin Cyber, a partner of Titania. “Titania’s new software capability will enable organizations to analyze their entire network infrastructure estate, accurately prioritize non-compliances, and take remediation action based on risk. They can now even do this on a continuous basis.”

The new software capability also enables federal organizations to:

- Drill down to NIST SP 800-53 controls and control enhancements with automated pass/fail evidence of compliance;
- Automate accurate configuration risk assessment, prioritization and mapping to NIST SP 800-53 based on DISA STIG risk categories and control correlation identifiers.
- Prioritize risk remediation actions for each non-compliance detected which can be used to

automate trouble-ticketing; and

- Proactively re-assess risk to ensure it has been mitigated and devices are secure to NIST SP 800-53 standards.

“We’re working closely with GRC and Security Operations providers to close the automation gap even more, so that our risk-prioritized remediation advice is linked to automated trouble-ticketing and remediation orchestration, and then proactively checked in Nipper Enterprise to ensure the changes have addressed the compliance issue, without opening up any further network gaps,” stated Ian Robinson, Chief Architect at Titania. “Closing the remediation loop has always been our aim, and our new evidence-based reports demonstrate how compliance posture can be significantly improved in significantly less time, with this approach.”

The new NIST SP 800-53 report is available in both the Nipper Enterprise solution which is used by security operations centers (SOCs) to continuously assure compliance, and Titania’s on-demand solution, Nipper, which is used by internal and external auditors and assessors.

Availability

Titania Nipper and Nipper Enterprise are available today. Additional evidence-based reports available in Nipper and Nipper Enterprise include DISA STIGs. PCI DSS 4.0, CMMC, and NIST SP 800-171 are expected in the coming months.

Nipper Enterprise also offers MITRE ATT&CK based incident prevention, forensics and response automation to improve attack surface management posture.
Visit titania.com to learn more.

About Titania

Based in the UK and Arlington, VA, Titania delivers essential cybersecurity automation software to thousands of organizations, including 30+ federal agencies within the US government, global telcos, multinational financial institutions, and the world’s largest oil and gas companies. Specializing in the automated security and compliance risk assessment and remediation for networking devices – routers, switches and firewalls – Titania helps organizations defend their networks from preventable attacks by identifying exploitable configuration drift and prioritizing the remediation of their most critical risks first. The company is best known for its award-winning solution, Nipper, which also overlays its security risk findings onto RMF assessments to assure compliance for CDM, DISA RMF, NIST, CMMC, and PCI DSS. To meet the growing market need for continuous accurate risk and remediation prioritized assessments, Titania has scaled Nipper for enterprises to support their zero trust security strategies. Visit Titania at www.titania.com

For more information, please contact:

Beth Fichtel/Cassandra Hegarty
CCgroup
+1 914-588-2695
Titania@ccgrouppr.com
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/657810312