TITANIA | Use case titania.com

Assure the security of your Operational Technology

Tackle the biggest risk to OT security with Nipper OmniSight

NIPPER OmniSight

Shut down critical vulnerabilities and misconfigurations in the routers, switches, and firewalls that connect and protect your Operational Technology (OT) environments, so there is no way through for attackers.

Use Nipper OmniSight to ensure network devices are hardened to vendor recommended standards; control gaps and rule conflicts are addressed; and your vital segmentation policies are being correctly enforced by every single device.

- **Identifies risks to OT that other tools miss and presents them via an intuitive dashboard**
- **Zero Trust segmentation and air-gapping assurance to confirm OT is protected**
- **Assesses configuration files, with no need for direct contact with devices**
- **Attack surface analysis to help prioritize risks and remediation**
- **CMDB centric: strengthens resilience and enables faster recovery**
- **Based on technology used by more than 100 elite cyber teams in energy and utilities, manufacturing and distribution, and national security.**

Assuring the network to enhance OT security

Cyber attackers thrive on both disruption and the threat of it – and disrupting operational technology is now a key target.

Business interruption costs from security incidents in OT amount to billions each year, with even the shortest break in operations incurring a high price. That then encourages ransomware groups, confident that many affected organizations will rapidly agree to pay.

But it's not just financial risks; there are major societal and economic ones too. State-backed and terror groups have been known to focus on disrupting the systems that ensure critical infrastructure functions safely.

Tackling the biggest risk to OT security / Assuring the network to enhance OT security

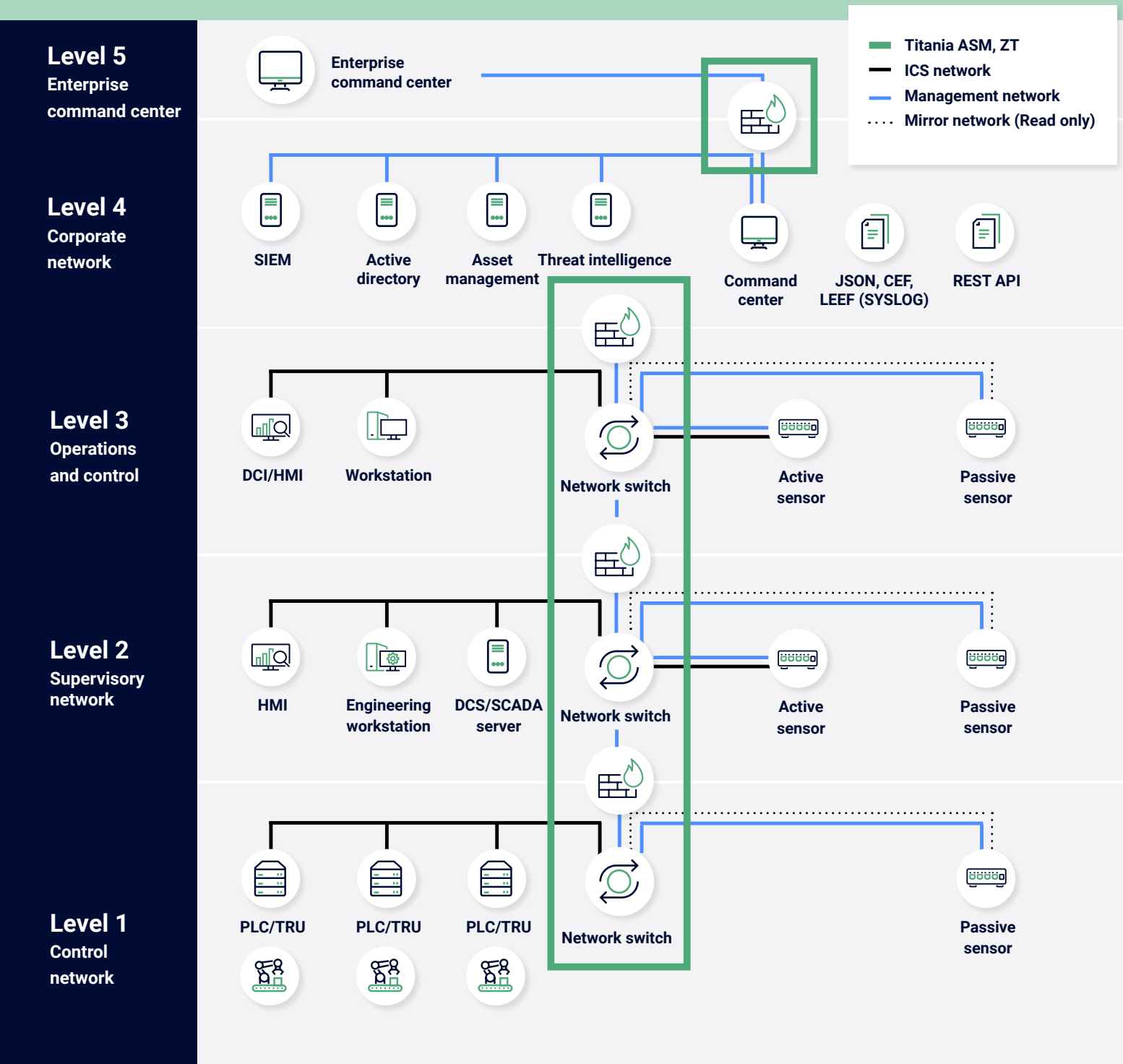
Complex industrial control systems are often powered by technology that was not designed with security in mind. These bespoke legacy platforms once operated well out of reach, but are now integrated with wider operations through conventional networking technology that organizations have paid little attention to. The result is that they often do not know what routers, switches and firewalls exist in their OT networks, or how those assets are truly configured. This is precisely where OT can be most vulnerable.

These devices are responsible for enforcing segmentation, access control and trust boundaries. So when these devices are not configured securely and intelligently segmented, they offer a tried-and-tested route in for attackers and security assumptions break down. Once inside the network, adversaries are able to move laterally and persist – gathering information, rerouting traffic, changing permissions or, worst of all, actively disrupting industrial systems.

Put simply, if the network devices that connect and protect your OT aren't verifiably secure, your operations aren't secure.

Purdue-aligned OT architecture

The role of network infrastructure in visibility and security.



How Nipper OmniSight can help

Nipper OmniSight gives OT operators confidence in their network security. Instead of simply hoping that policies are being followed, it confirms whether network devices – routers, switches and firewalls – are configured correctly and operating in accordance with your key security policies, like Zero Trust segmentation.

Where it identifies misconfigurations, it prioritizes them, in terms of risk – not only to OT network segments, but to your wider IT enterprise.

It also provides clear remediation guidance to ensure that devices are hardened to vendor recommendations, policies are enforced as intended, and exploitable control gaps or conflicts – including in air-gapped networks – are eliminated.

Answers are provided fast and at scale: Nipper OmniSight (Continuous) can assess 250,000 network devices in 24 hours. What's more, beyond point-in-time assessments, you can use it to monitor networks 24x7 and alert you to every device configuration change: users, rules, permissions. That way you can check whether changes are authorized and whether they leave key assets exposed.

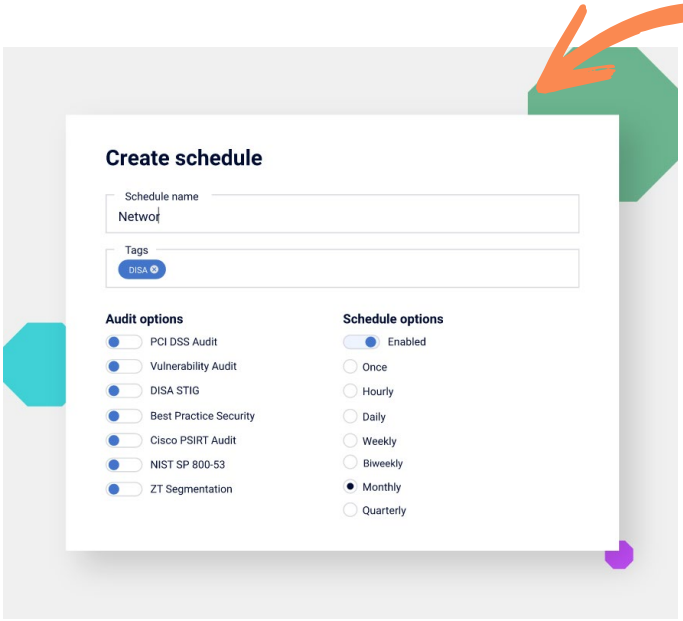
How it works

Nipper OmniSight uses configuration files to build a behaviorally accurate model of each device under assessment – meaning there is no interruption to the live environment.

It then runs more than 200 penetration tests on each device model, replicating the approaches attackers might take, to pinpoint misconfigurations and control gaps, and check whether the device is operating in line with your documented segmentation policies.

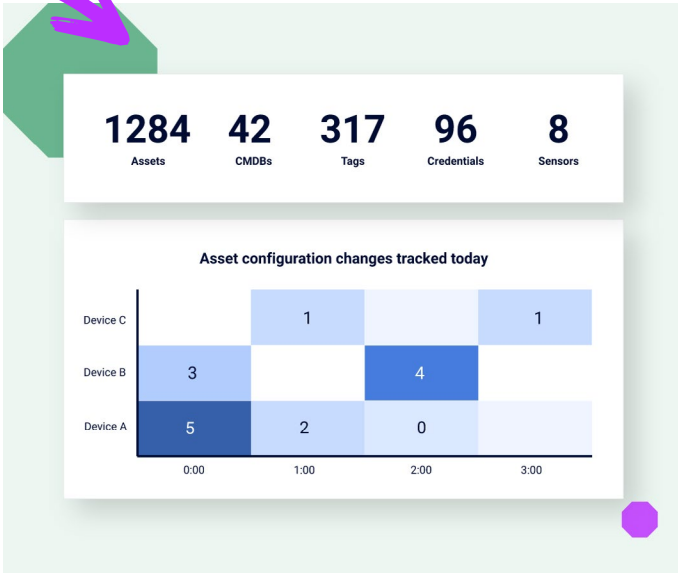
Exposures are mapped against the latest known exploitable vulnerabilities (KEVs) and MITRE ATT&CK data to prioritize the most urgent risks to business-critical segments and the enterprise. Risk scoring also factors in how easily a particular vulnerability can be exploited. The output is a comprehensive list of issues, with the most serious shown first. Given the potential for disruption, cyber risks to OT can be appropriately prioritized.

With **Nipper OmniSight (Standalone),** after uploading the configuration files for the devices in scope, run an assessment to receive a comprehensive point-of-time analysis that can inform a policy review, segmentation strategy or focused remediation effort.



Nipper OmniSight (Integrated) draws data from an existing configuration management database (CMDB) to conduct the initial analysis. It then allows you to schedule regular reassessments to identify and understand the impacts of configuration drift.

In **Nipper OmniSight (Continuous),** the built-in configuration collector will populate a CMDB with the live running configuration for every network device, and then monitor your networks on an ongoing basis for any change.



Supporting disaster recovery

Nipper OmniSight (Continuous) enables disaster recovery by maintaining a trusted configuration baseline and historical change record that teams can use to identify unauthorized or destabilizing changes, compare pre- and post-incident states, and restore devices to safer known configurations.

Continuous assessment of drift, policy-breaking change, and control weakness also helps reduce recovery time by improving root-cause analysis and supporting more precise remediation.

About Nipper OmniSight

Titania Nipper solutions provide high-assurance, configuration-centric security for the routers, switches, firewalls, SD-WAN devices, and wireless access points (WAPs) that underpin every business-critical network.

Nipper OmniSight provides enterprise-scale exposure visibility – offering scheduled or continuous assessment, change detection, asset discovery, segmentation validation, APT-relevant configuration insight and Zero Trust-aligned reporting.

Routers

Switches

Firewalls

SD-WAN devices

Wireless access points (WAPs)

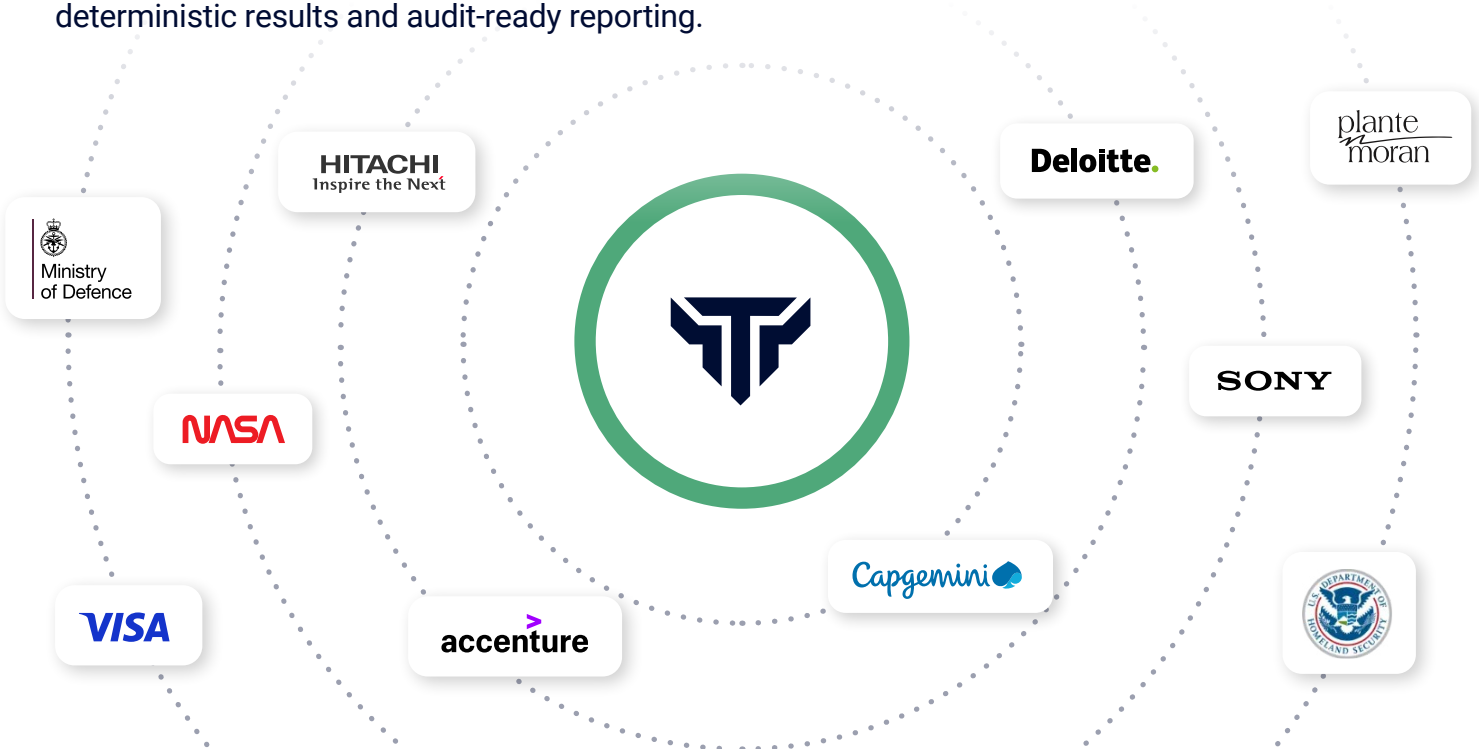
Dedicated to securing the networks society depends on

Titania's cybersecurity software helps governments, defense, critical infrastructure and enterprises reduce risk by finding configuration-level exposures attackers exploit.

Built on a penetration testing approach, delivered at speed and scale, Nipper solutions equip security and network leaders to stay ahead of AI-accelerated adversaries and Advanced Persistent Threats (APTs) – with deterministic results and audit-ready reporting.

Our portfolio supports teams at every stage – from point-in-time assessment and hardening to ongoing monitoring as environments change.

Headquartered in the UK with operations in Arlington, VA, Nipper solutions are trusted by thousands of global enterprises including 30+ U.S. federal agencies, major financial institutions, telecommunications providers, and leading oil and gas companies.



Seeing is believing

Nipper OmniSight is built on our proprietary virtual device modelling technology that is already used by more than 100 elite cyber teams worldwide. We'd love to show you how it can work for yours and assure the security of your OT.

To arrange a demo, or speak to one of our experts

USA
2451 Crystal Dr, Suite 600
Arlington, VA 22202
enquiries@titania.com

UK
167-169 Great Portland Street,
London, England, W1W 5PF
enquiries@titania.com

Learn more about how Titania can protect your Operational Technology (OT) environments

titania.com/solutions/industry