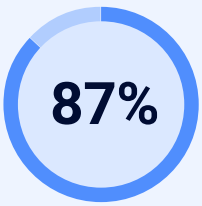
TITANIA

titania.com

From threat chasing to proactive defense: why organizations must target and fix their exposure to critical network threats

The Middle East is facing an alarming surge in the number and diversity of cyber-attacks, and the stakes could not be higher.

Public and private sector organizations must protect the assets that power economies and communities. Yet, while regional digital transformation accelerates, the exposure to cyber threats has grown just as rapidly.

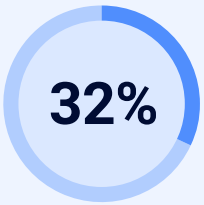


increase in ransomware attacks against industrial organizations

2025 OT/ICS Cybersecurity report - Dragos

the average cost of a data breach in the region, almost double the global average

Cost of a Data Breach Report 2025 - IBM



of all cyber attacks were conducted by Advanced Persistent Threat (APT) groups

Positive Technologies study

While ransomware, zero-day, and AI-generated attacks dominate headlines, many organizations overlook the number one initial attack vector: the exploitation of a vulnerability or misconfiguration.

These reside hidden deep within the network - unseen by conventional cybersecurity solutions.

of vulnerabilities reside deep within the network

2025 OT/ICS Cybersecurity report - Dragos

of devices with the most dangerous vulnerabilities are routers

Riskiest Connected Devices of 2025 report - Forescout

source of cybersecurity misconfigurations is default configurations of software and applications

NSA and CISA

With tens of thousands of identified vulnerabilities, network and security teams are caught in a reactive cycle of endless vulnerability alerts and patching demands.

CNI: a high-impact target for APTs

Geopolitics is increasingly playing out in cyberspace through state-backed sabotage campaigns targeting energy, transportation and telecoms networks.

Microsoft reports that 38% of network disruptions in the Middle East were linked to nation-state actors, such as APT34, APT33, Volt Typhoon, Earth Esteries, Beserk Bear and Cosy Bear – as well as regional hacktivists.

Recent global advisories also confirm that the Salt Typhoon group has penetrated telecommunications providers in 80 countries, exploiting routers to move laterally and exfiltrate sensitive data, underscoring that network devices are high-value targets.

The nature of these attacks has shifted from smash-and-grab ransomware to long-term, stealthy compromise using Living off the Land (LOTL) tactics.

These adversaries are not just stealing data; they are embedding themselves to **disrupt, degrade, or destabilize** networks over time.

Ransomware and the rise of AI-powered threats

A major new concern is the emergence of Charon ransomware, which targets the Middle East's public sector and aviation industry using APT-style evasion tactics.

In the first half of 2025 alone, over 90 unique data leaks from Gulf-based organizations were recorded on dark web sites, affecting industries from oil and gas to healthcare.

Attackers are also changing their deployment strategies. Instead of encrypting one machine at a time, automated ransomware variants now spread as far as possible before executing simultaneously across the network, causing catastrophic disruption without warning.

The rapid rise of AI has increased the urgency. Attackers now use AI tools to exploit vulnerabilities more efficiently. Gartner predicts that by 2027, AI agents will halve the time it takes attackers to exploit account exposures.

While AI accelerates the speed and scale of attacks, it doesn't invent new infiltration methods. Ransomware exploits the same vulnerabilities and misconfigurations related to privileged escalation and lateral movement.

A foundational step in defending against ransomware is implementing macro-segmentation – isolating mission-critical systems from general IT infrastructure. This limits the ability of an attacker to move laterally across the network and reduces the scale of the attack.

More importantly, macro-segmentation enables risk-based prioritization. When segments are aligned with operational importance, network and security teams can mitigate threats based on potential impact, not just a generic severity score.

The hidden cost of 'Threat Debt'

Threat debt is the cumulative cost of not addressing foundational risks, specifically the misconfigurations that quietly enable hundreds of common vulnerabilities and exposures (CVEs) over time.

While threats constantly evolve to evade detection, they fundamentally look for the same vulnerabilities. By fixing these root-cause issues, you not only retire current threat debt but also prevent future exploits.

For example, one secure configuration can neutralize dozens of future CVEs. The ROI on foundational security is the breach that doesn't happen and the brand reputation you don't have to rebuild.

Foundational security builds operational resilience

New regulations in the Middle East and across the globe – like the EU's DORA and NIS2 Directives place a strong focus on maintaining resilient operations during a cyber disruption. This means that annual audits of your network devices are no longer sufficient.

Real-time network visibility is essential to spot vulnerabilities early and maintain compliance. Because configuration drift happens fast, and you can't protect against every possible cybersecurity event. The goal should be to commit to tackling the exposures that most threaten your business.

By mapping configuration assessments to MITRE ATT&CK tactics, techniques, and procedures (TTPs) and onto relevant attack vectors like APT34 aka 'OilRig', network and security teams can visualize vulnerabilities from an attacker's perspective and prioritize remediation based on threat models.

Combining automated risk exposure monitoring with network segmentation insights allows you to focus efforts on the most critical exposures, dramatically reducing the attack surface.

Network readiness is not optional; it's the new baseline. The question is no longer "Are we compliant?" but "Are we ready?"

Phil Lewis

Senior Vice President - Market Strategy and Development, Titania

With a proven track record in Strategic Risk Management. Phil Lewis is now championing Titania's global expansion at the forefront of network readiness, recovery and resilience automation.
