New Titania Research Reveals Surge in Proactive Security Investments

Over 70% of businesses have increased spending on proactive security solutions, outpacing both preventative and reactive measures

ARLINGTON, VA, UNITED STATES, June 18, 2024 /EINPresswire.com/ -- Titania, specialists in continuous network security and compliance assurance solutions, today announced the release of compelling new research that highlights a significant shift in cybersecurity spending towards proactive security measures. The report, Emerging Best Practice in the use of Proactive Security Solutions, indicates a marked increase in investments aimed at preemptively mitigating cyber threats. In fact, 70% of businesses reported increased spending on proactive security solutions, such as attack surface management and risk-based vulnerability management, over the past year. This notably outpaces investments in both preventative and reactive measures.

The study, completed in partnership with Omdia, a global analyst and advisory leader, surveyed over 400 security decision-makers in North America, the UK, France, and Germany. It underscores the acceleration in adoption of proactive security measures from three key drivers: 'reducing the opportunity for threats', 'reducing the mean time to remediate known vulnerabilities', and 'minimizing attack surface'. The facts suggest that proactive security solutions are not just an additional layer of protection but are integral to a comprehensive understanding of the relevant threat landscape and attack surface, which will help organizations improve both operational resilience and readiness.

Key findings of the report include:

· Strategic Implementation: A significant portion of organizations, particularly those with mature security postures, are strategically deploying proactive security solutions. This trend is especially prevalent among larger organizations. This growth is particularly pronounced in EMEA, where 74% of respondents increased their budgets, compared to 67% in North America. The desire is particularly strong amongst financial services organizations (54%) and critical infrastructure organizations (53%) including energy and utilities companies.

In addition, almost half (47%) reported that their top cybersecurity goals for the next 12-24 months are to reduce the opportunity for threats with proactive security. Conversely, only 27% of organizations plan to improve tactical outcomes, such as better threat prevention, detection and response.

· Enhanced Security Posture: Respondents report a strong desire to improve security posture and expect that the broader integration of proactive security tools will greatly improve attack surface management and security control optimization. Currently, a large majority of respondents report having limited visibility into the security posture of network assets (firewalls, switches and routers) and long cadences between assessments – with roughly half of organizations checking network devices at most, monthly. Organizations are also much more likely to only monitor all devices in critical segments (or simply look at a sample of devices), than to monitor every device in their networks. Notably, critical infrastructure organizations (i.e., energy, utilities, and transportation) report much lower confidence than other industries in their ability to maintain adequate network segmentation and prevent unauthorized access to networks.

· Disruption Anticipation: Almost half (48%) of all respondents anticipate a high level of organizational disruption due to the broader adoption of proactive security solutions, highlighting the transformative impact these measures are expected to have.

“This research vividly illustrates a widespread and rapid shift towards proactive security to improve operational readiness and resilience. Organizations are recognizing the critical need to stay ahead of known threats and shut down attacks by investing in solutions that offer real-time visibility of their security posture and remediating action that will continuously minimize their exposure,” said Tom Beese, Executive Chairman, Titania.

When it comes to the importance of consolidating proactive security tools, businesses indicated that better visibility and management of the attack surface (65%), improved security control optimization (60%), and manpower productivity improvements (54%) were the most crucial.

The survey also identified the most critical proactive security capabilities as the ability to view risks through different attack frameworks (61%), full asset context (60%), and integration with existing security fabric to implement temporary mitigations (57%).

“While the cybersecurity industry has clung to the “assume breach” mantra with its preventative and reactive solutions, organizations are awakening to a smarter strategy: proactively understanding attack surfaces, mapping attack paths, and plugging vulnerabilities to prevent breaches. While a host of standalone proactive tools have been available for many years, proactive security platforms are emerging that can provide much more holistic risk discovery, prioritization, and automated remediation”, Andrew Braunberg, Principal Analyst at Omdia, explains in the research.

For example, network device configurations are an important component of security posture management. The need to correctly configure network devices, particularly externally facing devices, in a secure state (and then maintain that state) is a critical component of attack surface reduction and effective risk management – and underpins a proactive security approach.

Data from this research highlights high confidence levels in the security capabilities of network devices such as firewalls, routers, and switches, and the paradox of poor assessment practices limiting the visibility many organizations have into these assets. For example, the data reveals that making risk assessments proactively after configuration changes is clearly not yet common practice; 6% of financial services organizations report proactively assessing their firewalls, and only 4% proactively assess their switches, or routers. Indicating adoption of proactive security solutions that automate and close the loop on proactive configuration assessments would have a transformative impact.

“There is currently a limited amount of industry guidance on best practice when building a proactive security strategy. But the report highlights that the US Defense Department Command Cyber Readiness Inspection program (CORA) and the EU’s Digital Operational Resilience Act (DORA) requirements map well to end-user requirements for proactive security solutions, making it impossible to imagine meeting these regulations and benefitting from the full potential of a proactive security approach without embracing configuration security automation,” continued Beese. To access the full report, please visit https://www.titania.com/proactive-security-solutions. This study was completed in Q1 2024 with Omdia who surveyed 405 security decision makers in North America, the UK, France, and Germany.

Beth Fichtel/Cassandra Hegarty
CCgroup
titania@ccgrouppr.com
