Media Contact:
Trend Micro Communications
817-522-7911
media_relations@trendmicro.com

Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response

Trend Micro reveals over half of Security Operation Centers are overrun with redundant security tools

DALLAS, 12th October 2021 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today revealed that global organizations have on average 29 security monitoring solutions in place, complicating Security Operations Center (SOC) efforts to prioritize alerts and manage cyber risk effectively.

The global independent research* uncovered serious challenges facing SOC teams tasked with detecting and responding to emerging cyber threats. Those defending organizations with more than 10,000 employees have an average of almost 46 monitoring tools in place.

Half (51%) of respondents claimed they no longer use many of these tools for reasons including:

- Lack of integration (42%)
- Lack of skilled professionals (39%)
- Difficulty understanding how to operationalize them (38%)
- Out of date (37%)
- Don't trust them (20%)

The potential cost of these challenges is high: Respondents said that, on average, their organization stands to lose over $235,000 if they fall foul of the GDPR due to an incident.

"Tool sprawl is increasingly common in global organizations of all sizes, but when it comes to incident detection and response, there's a growing but sometimes unacknowledged cost associated," said Trend Micro's Technical Director (UK) Bharat Mistry.

The research also found that 92% of respondents have considered managed services to outsource their detection and response capabilities. These service-based offerings typically can help to overcome in-house skills challenges, providing a single, unified version of the truth to drive improved incident response.

"Not only do organizations have to pay for licensing and maintenance, but SOC teams are increasingly stressed to the point of burnout trying to manage multiple solutions. Being unable to prioritize alerts may also expose the organization to breaches. It's no surprise that many are turning to SOC-as-a-Service," added Mistry.

***Research methodology**

The study is based on interviews with 2,303 IT security decision makers in 21 countries. This includes leaders who run SOC teams (85%) and those who manage SecOps from within their IT security team (15%). All respondents came from 250+ employee companies.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.