70% Of SOC Teams Emotionally Overwhelmed By Security Alert Volume

Trend Micro study reveals the human cost of underpowered Security Operations Centers

DALLAS, May 25, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released results from a new study that reveals SOC and IT security teams are suffering from high levels of stress outside of the working day—with alert overload a prime culprit.

According to the study, which polled 2,303 IT security and SOC decision makers across companies of all sizes and verticals, 70% of respondents say their home lives are being emotionally impacted by their work managing IT threat alerts. This comes as the majority (51%) feel their team is being overwhelmed by the volume of alerts and 55% admit that they aren't entirely confident in their ability to prioritize and respond to them. It's no wonder therefore that teams are spending as much as 27% of their time dealing with false positives.

These finding are corroborated by a recent Forrester[1] study, which found that "security teams are heavily understaffed when it comes to incident response, even as they face more attacks. Security operations centers (SOCs) need a more-effective method of detection and response; thus, XDR takes a dramatically different approach to other tools on the market today."

Outside of work, the high volumes of alerts leave many SOC managers unable to switch off or relax, and irritable with friends and family. Inside work, they cause individuals to turn off alerts (43% do so occasionally or frequently), walk away from their computer (43%), hope another team member will step in (50%), or ignore what is coming in entirely (40%).

"We're used to cybersecurity being described in terms of people, process and technology" said Dr. Victoria Baines, Cybersecurity Researcher and Author. "All too often, though, people are portrayed as a vulnerability rather than an asset, and technical defenses are prioritized over human resilience. It's high time we renewed our investment in our human security assets. That means looking after our colleagues and teams, and ensuring they have tools that allow them to focus on what humans do best."

With a staggering 74% of respondents already dealing with a breach or expecting one within the year, and the estimated average cost per breach USD$235,000, the consequences of such actions could be disastrous.

"SOC team members play a crucial role on the cyber frontline, managing and responding to threat alerts to keep their organizations safe from potentially catastrophic breaches. But as this research shows, that pressure sometimes comes at an enormous personal cost," said Bharat Mistry, technical director for Trend Micro. "To avoid losing their best people to burnout, organizations must look to more sophisticated threat detection and response platforms that can intelligently correlate and prioritize alerts. This will not only improve overall protection but also enhance analyst productivity and job satisfaction levels."

Trend Micro Vision One is the company's answer to the struggles of SOC teams. Prioritized, correlated alerts using data from the entire IT environment help teams spend their time more wisely. Fewer alerts and stronger intelligence allow teams to regain balance in their work life and ease the emotional toll of security.

To find out more, please read the accompanying report by visiting:https://www.trendmicro.com/explore/en_gb_soc-research.

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.

[1] Allie Mellen, Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR (Forrester, 2021)

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

Additional assets available online: Photos (1)

https://newsroom.trendmicro.com/2021-05-25-70-Of-SOC-Teams-Emotionally-Overwhelmed-By-Security-Alert-Volume