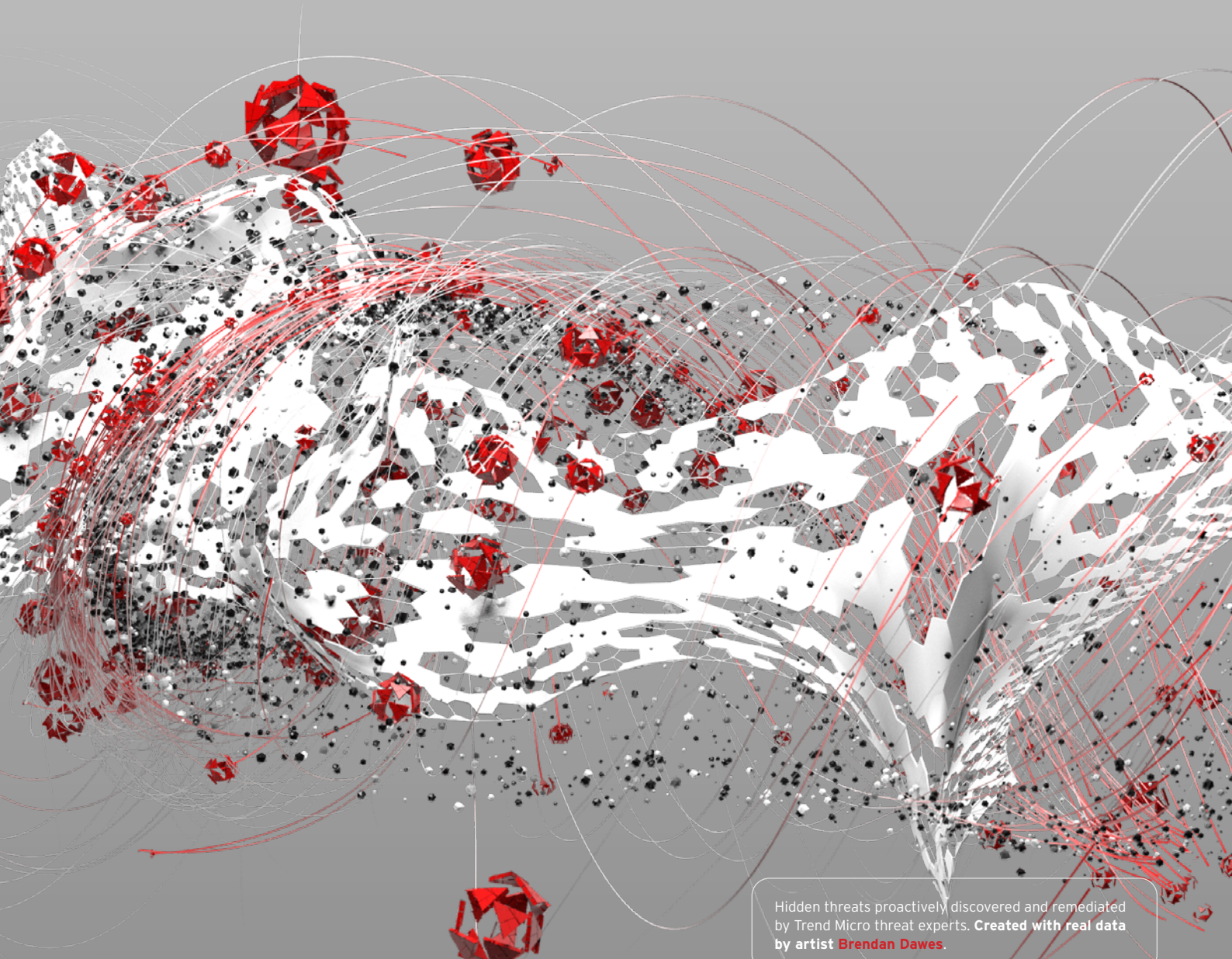


A global study  
**SECURITY OPERATIONS  
ON THE BACKFOOT:**

How poor tooling is taking its toll on  
security analysts



Hidden threats proactively discovered and remediated  
by Trend Micro threat experts. Created with real data  
by artist **Brendan Dawes**.

Over recent years, security and business leaders have had to modify their expectations of what effective cybersecurity can achieve. Long gone are the days when all resources were poured into protecting the corporate network perimeter. Thanks to widespread adoption of cloud infrastructure and services, BYOD and now mass remote working, that perimeter is far more fluid, flexible and porous.

Threat actors can and regularly do sneak into corporate networks today with stolen, phished or cracked credentials, or by exploiting unpatched vulnerabilities—of which there are many to choose from. This means CISOs and CEOs must accept that their organization will be breached, or might already have been. The key is finding those attackers before they have a chance to cause serious damage.

This is where the Security Operations Center (SOC) comes into its own. The function offers a centralized, always-on hub for monitoring, detecting and responding to cyber-threats. In theory, it should be an effective way to manage the growing risks associated with threat activity. In reality, many teams are struggling to provide the support CISOs expect of them, and are suffering as a result not just at work, but also in their private lives.

*To find out more, Trend Micro commissioned a new global study, 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, with the exceptions of Norway (10+), Denmark (25+), Austria and Belgium (both 100+).*



**2,303**

IT security decision makers



**21**

countries

**85%** includes leaders who run SOC teams



**250+**

employee companies



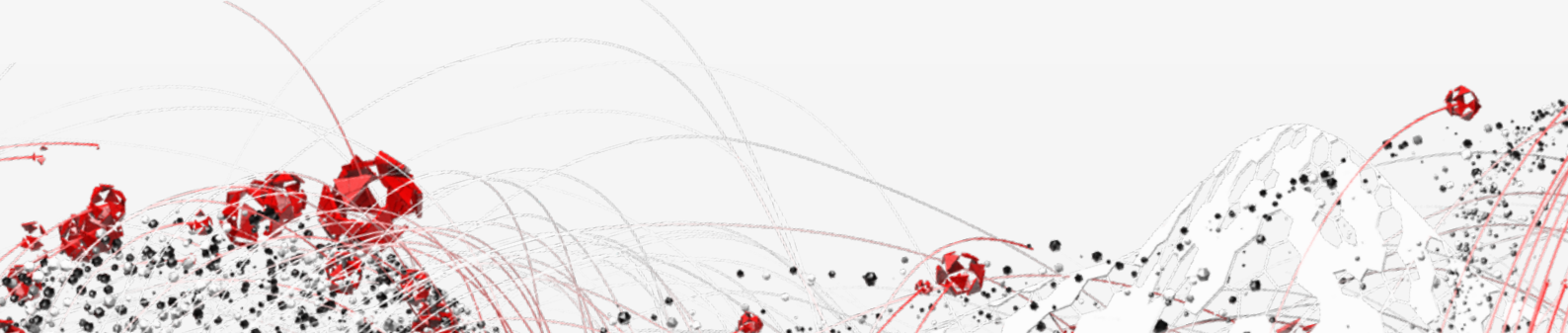
# Breaches are happening

Some 85% of global organisations now boast a SOC. This is a positive development in the fight against cybercrime. Ideally, they should be working 24/7/365, as global threat actors never sleep, although we found only 45% do so at present.

Let's be clear about the scale of the challenge facing SecOps teams. We found that three-quarters (74%) of respondents are already dealing with a breach or expecting one within the year. This doesn't necessarily mean that they're failing at their job—as discussed, the key is to react quickly to initial breaches to ensure the threat actors can't make their way to sensitive data stores or other vital assets. However, it does illustrate the level of threat activity facing SecOps teams.

These are high-pressure incidents. Unlike the day-to-day roles of most employees, security professionals engaged in threat detection and response have hanging over them the continuous concern that if they fail, the organization could suffer serious financial and reputational damage. Respondents estimated an average cost per GDPR breach at \$235,000, but in reality it could be much higher. Some corporate ransomware victims have disclosed losses in the tens of millions of dollars, for example.

Some of the key factors making SecOps problematic today include:

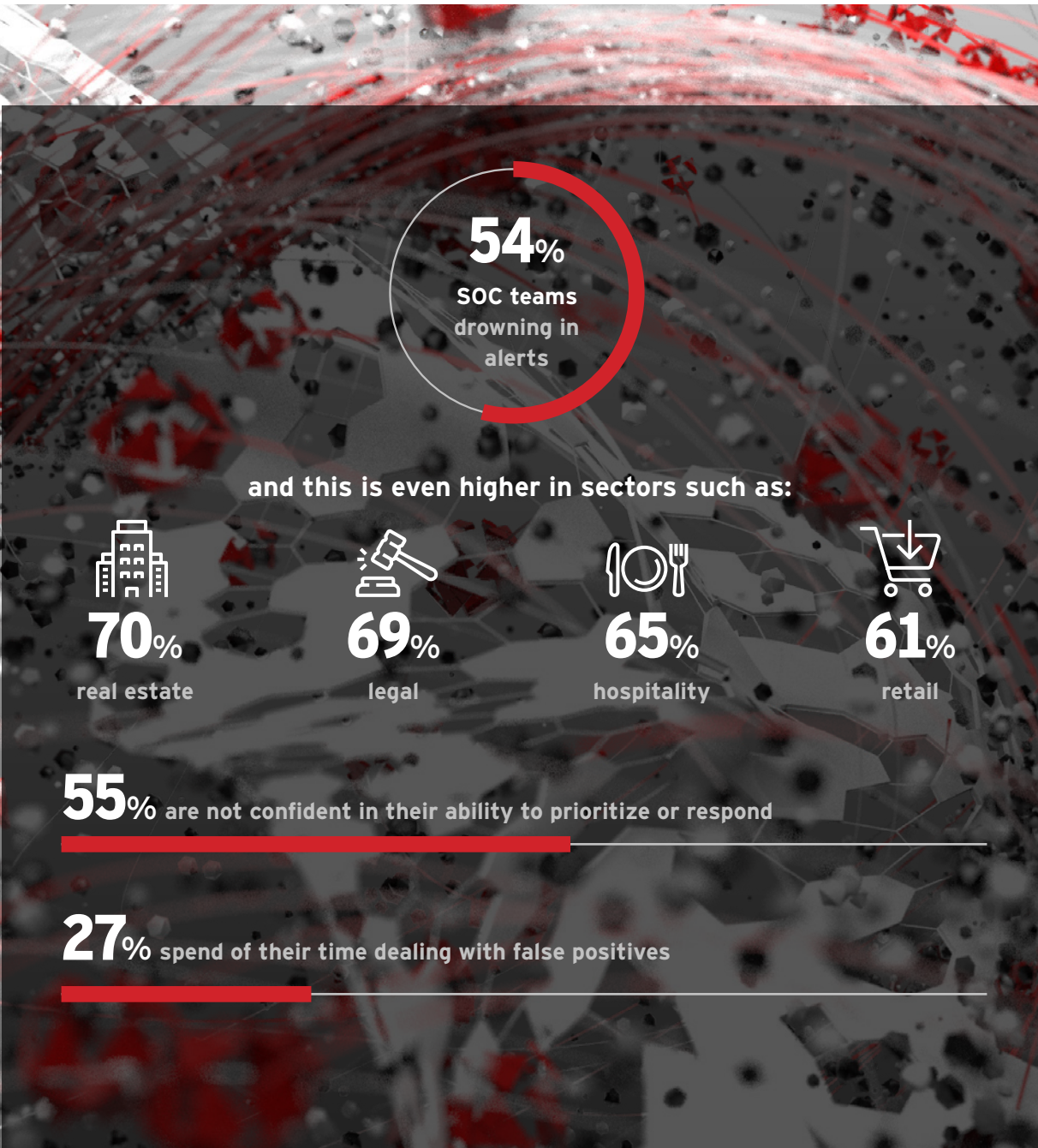
- **A ransomware epidemic:** Thanks to the popularity of the affiliate model and the use of increasingly targeted and sophisticated tactics, which also include data exfiltration. Trend Micro detected a 34% year-on-year increase in new ransomware families in 2020
  - **Insider negligence:** As detailed in our Head in the Clouds research, home working has led to employees engaging in more risky behavior than they'd otherwise think is acceptable, such as uploading corporate data to unapproved apps
  - **Distributed working:** The mass shift to remote work has also impacted the productivity of SecOps teams used to working together in the office
  - **Use of legitimate tools:** Threat actors are increasingly leveraging legitimate system features and tools to perform lateral movement and data exfiltration, making them harder to spot
  - **Tool sprawl:** As we'll see, one of the main causes of SecOps pain is the sheer number of protection tools now in use across the enterprise, leading to an ever higher volume of alerts
- 

# SecOps overwhelmed by alerts

Our research revealed the global average for SOCs is 30 discrete security monitoring tools, and slightly fewer (28) in the UK. At the moment these cover mainly email and web and network-based products, but we expect these to be joined by EDR and SIEM in 2021.

The result of this tool sprawl, escalating threat levels and a dearth of technology to correlate and prioritize alerts—is that SecOps teams feel overwhelmed. Over half (51%) said they are drowning in alerts, dropping slightly (45%) in the UK. The figure increased to 54% for global SOC teams and even higher in sectors such as real estate (70%), legal (69%), hospitality (65%) and retail (61%).

Over half (55%) of respondents admitted they aren't confident in their ability to prioritize or respond to these alerts. So it's perhaps no surprise that they spend on average over a quarter (27%) of their time dealing with false positives (25% in the UK). An equal challenge stemming from this situation is the likelihood of false negatives—alerts from legitimate threats—sneaking in under the radar.



# Analysts are stressed out and unhappy

The bad news for SecOps managers is that this alert overload is having a material impact on the quality of life of their staff. Some 70% of respondents said they feel emotionally affected by their work. Many claimed that they:

- Are unable to relax due to stress
- Find their downtime ruined by their inability to switch off
- Are irritable with friends and family

Just 28% of SOC teams said they are able to fully switch off and forget about work after clocking off.

The number of alerts flooding the SecOps team is so great that large numbers of respondents have said that they've frequently or occasionally:

- Ignored alerts completely and worked on something else (40%)
- Walked away from the computer feeling overwhelmed (43%)
- Turned off alerts (43%)
- Just assumed an alert was a false positive (49%)
- Hoped another team member would step in to help (50%)

## Respondents admit to:

40%

ignoring alerts completely and working on something else

43%

walking away from the computer feeling overwhelmed

43%

turning off alerts

49%

assuming alerts were false positives

50%

hoping another team member would step in to help

# A better approach with Trend Micro Vision One™

Clearly these tensions are not only putting organizations at greater risk of succumbing to serious cyber-threats, but are also threatening the mental health and wellbeing of the security team.

The good news is that technology platforms exist which can take the pressure off SecOps teams by improving threat detection and response. Trend Micro Vision One is a purpose-built threat detection platform that goes beyond XDR to offer a prioritized view of, and accelerated response to, threats across the enterprise. Unlike many detection and response solutions that only look at the endpoint, Trend Micro Vision One correlates alerts across emails, servers, cloud workloads and networks for maximum visibility and intelligent response.

With Trend Micro Vision One your organization can benefit from:

- Faster time-to-detection and response, thanks to fewer, prioritized alerts flagged for action
- Comprehensive visibility and protection across the endpoints, networks, email, datacentre and cloud to automatically block attacks
- Automated remediation to remove malware and free-up analyst time
- A centralized source of alerts, investigations and containment, to support faster response with fewer resources
- Improved SOC analyst productivity
- Reduced exposure to financial and reputational risk
- Happier SecOps teams

With a platform like Trend Micro Vision One in place, organizations can respond to incidents faster to stop threat actors in their tracks before they're able to cause any lasting damage. And by helping SecOps prioritize alerts, they can reduce the risk of analyst burnout, improve job satisfaction and enhance productivity.

To find out more, head to [www.trendmicro.com](https://www.trendmicro.com) or [take a virtual test drive](#).

Copyright © 2021 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, and the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be company logos or registered trademarks of their owners. Information contained in this document is subject to change without notice.

