opentext™

POINT OF VIEW

Have confidence that your SOC's threat teams are catching advanced threats faster and with greater accuracy

Find threats that matter, faster

Industry backdrop

As the last line of defense protecting your company against cyberthreats, security operations centers (SOCs) are fighting an increasingly complex war. Insider threats lurk within company walls, while novel attacks and advanced persistent threats (APTs) attack from the outside. Alert fatigue, persistent skills shortages, and resource constraints further compound the challenge of defending your company against cyberthreats.

Insider threats

Insider cyber threats are a significant and growing concern for organizations in every industry. Whether the intent is inadvertent or malicious, individuals within an organization who have authorized access to systems, networks, and sensitive data pose a significant threat. A recent study by Elevate Security revealed that 8% of employees were responsible for 80% of security-threatening mistakes.[1]

Novel attacks

Attackers find vulnerabilities, bypass defenses, or compromise systems using constantly evolving methods and techniques to exploit technology, processes, and human behavior. This rapid evolution of cyberthreats demands continuous adaptation. SOCs must stay updated on emerging attack vectors and tactics to effectively detect and mitigate new threats. For example, in just a two-month period between March and May 2023, threat actors launched an average of 11.5 attacks and introduced approximately 1.7 new malware samples each minute.[2]

Advanced persistent threats (APTs)

APTs are particularly dangerous, as they infiltrate networks stealthily, remain undetected for months, and relentlessly target your most critical data and operations. These sophisticated threats are backed by advanced tactics and well-funded attackers, making them a serious risk to any organization. And detecting them is challenging due to their stealthy nature and the difficulty in attributing anomalous behavior to such APT activity. A growing recognition of the importance of these threats has led to increased investment. By 2027, spending in the advanced persistent threat protection market is expected to reach $18.6 billion.[3]

1 Forbes, *4 Formidable Cyberthreats Every Employee Should Know,* 2024
2 The Hacker News, *Malware Unleashed: Public Sector Hit in Sudden Surge, Reveals New Report,* 2024
3 National Defense Magazine, *Containing Rise of Advanced Persistent Threats,* 2024

Alert fatigue

SOCs often deal with an overwhelming number of security alerts, and more than 59% of cybersecurity professionals reported receiving more than 500 cloud security alerts each day.[4] This can lead to SOCs missing critical threats.

Skills shortage

There is a notable shortage of skilled cybersecurity professionals and it is impacting the effectiveness of SOC operations. The global cybersecurity workforce gap reached a new high, with an estimated 4.8 million professionals needed to effectively secure organizations, a 19% year-on-year increase.[5]

Resource constraints

Limited resources can hinder the SOC's ability to implement comprehensive security measures and maintain round-the-clock vigilance. The majority of CISOs—80%—report that they do not have sufficient funding to implement robust cybersecurity measures.[6]

Addressing these challenges requires a multifaceted approach, including advanced threat detection technologies, continuous staff training, and robust incident response strategies.

More than

59%

of cybersecurity professionals reported receiving more than 500 cloud security alerts each day.[5]

The majority of CISOs—

80%

report that they do not have sufficient funding to implement robust cybersecurity measures.[7]

4 Security Magazine, *One-fifth of cybersecurity alerts are false positives,* 2022
5 ISC2, *Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists,* 2024
6 SOCRadar, *CISO Top 10 Statistics and Trends,* 2024

The OpenText approach

The threat landscape is becoming more complex due to increasing volume, frequency, and level of sophistication, and this has been compounded by the advent of generative AI. Traditional rule-based detection tools, adept at finding known threats are being pushed to the limit by emerging attacks for which there are not yet rules in place.

At OpenText we partner with security operations teams to elevate their cybersecurity maturity level in a cost-effective and non-disruptive manner. Our approach is anchored by four key principles:

1. Enable threat detection that matters:

Without robust detection, effective response is impossible. OpenText™ Core Threat Detection and Response proactively adapts to your unique environment, continuously refining baselines to uncover elusive insider threats, novel attacks, and advanced persistent threats—all while reducing false positives. This adaptive approach ensures your SOC can detect what truly matters before incidents escalate.

2. Enhance existing security posture:

Unlike competitors that often require extensive reconfiguration or additional infrastructure, OpenText Core Threat Detection and Response is engineered to integrate into your existing environment. Instead of displacing or duplicating your current investments, we complement them—streamlining workflows, improving detection accuracy, and providing the adaptability and scalability needed as your security architecture evolves. The result is a more cohesive, effective security posture that builds on what you already have, without adding unnecessary complexity or overhead.

3. Deliver tangible value:

- **Find threats others miss:** Our advanced and patented (10+) behavioral analytics powered by 100% online machine learning, reveals hidden threats that evade traditional (rule based) tools, giving organizations early and actionable detection capabilities.
- **Reduce alert fatigue:** OpenText Core Threat Detection and Response uses behavioral risk scoring to prioritize threats, reducing alert overload and ensuring the team focuses on high-risk activities first.
- **Ease of use and lower overhead:** Dynamic detection automatically evolves with a changing environment and eliminates the need for manual adjustments that are prevalent in other tools. Cybersecurity Aviator interprets and translates high volumes of complex security telemetry into plain language and delivers context-rich leads. OpenText helps automate threat hunting to boost operational efficiency.

4. Maximize success with expertise on tap:

The optimal combination of technology and users often leads to success. Not only are our battle-tested threat hunters skilled in our technology, they are also experts in finding some of the most difficult to find threats in the world. The experience gained through working with our global customers is invaluable in finding the threats that matter, faster. They provide a service that complements your existing operations and maximizes your technology investment.

Next steps and business outcomes

OpenText Core Threat Detection and Response paves the path to achieve advanced cybersecurity maturity, providing the optimal combination of technology and expert services to accelerate the transition without disruption to your current infrastructure.

Current state	Future state
Baseline protection for known threats and simple risks.	Contextual insights into your organization's unique normal and changing risk profile.
Fear of missing high impact unknown threats in the face of rapidly changing threat landscape.	Confidence in proven AI detecting unknown threats for which there are no rules.
Insider threats often go unnoticed for almost three months.	Reduce or eliminate remediation costs by detecting insider threats within days or hours.
Out-of-the box detection requiring time-consuming customization.	Threat detection optimally customized and automatically adapted to your threat environment.
Wasted human capital on low quality and inaccurate threat leads.	Maximize your human and technology investments.

OpenText Core Theat Detection and Response provides:

Core feature	Benefit
AI-driven advanced behavioral analytics	Automatically adapts to your changing business environment, detecting insider threats and rogue activities without additional configuration. Understands your organization's unique behavior to spot deviations that signal threats, helping prevent data breaches, IP theft, and malicious activity.
Seamless integration with Microsoft Defender for Endpoint and Entra ID	Integrates directly with Microsoft security tools like Defender for Endpoint and Entra ID, leveling up advanced threat detection by providing unique behavioral insights, enhanced risk context, and streamlined security operations.
Risk scoring for threat prioritization	Prioritizes high-risk threats like malicious insiders, with behavior-based risk scoring, reducing alert fatigue and helping teams focus on the most critical incidents in days or hours, not months.

How OpenText Threat Detection and Response addresses industry-specific challenges:

Industry	OpenText Core Threat Detection and Response
Financial services	Enables financial institutions to enhance their ability to protect client data, and prevent unauthorized access to sensitive information. With advanced behavior monitoring, banks and financial services can detect irregular user patterns, reducing the likelihood of insider threats and malicious intent.
Healthcare	Empowers security operations to strengthen protection of electronic health records (EHR) and to mitigate the risk of unauthorized access that could lead to HIPAA (or other) violations by identifying unusual access attempts or changes in behavior that could indicate insider threats, protecting patient privacy.
High tech	Elevates protection of sensitive IP and R&D data by detecting anomalous behavior and insider threats before intellectual property can be compromised. It enables high tech firms to safeguard proprietary information and maintain competitive advantage.
Retail and e-commerce	Reinforces protection of payment data and customer information from unauthorized access, while also preventing data breaches that could disrupt sales operations, by spotting suspicious employee activities to strengthen data integrity and secure transactions.
Manufacturing	Defends against unauthorized access to proprietary production data and systems, securing intellectual property and preventing costly operational disruptions caused by malicious insiders or cyberattacks.

Resources

Learn more about what OpenText Core Threat Detection and Response can do for your cyber defence or see it in action.

Learn more ›

opentext™