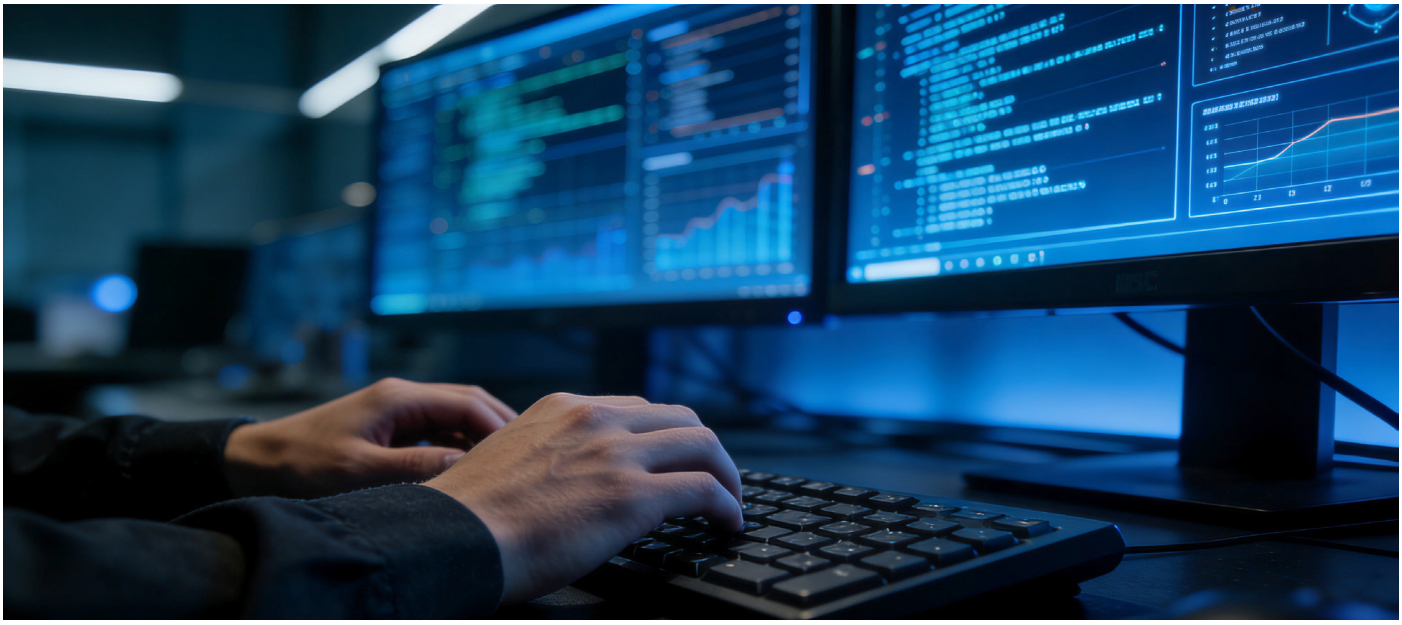
OpenText SIEM for preemptive threat detection

Automated, proactive, and holistic SecOps solution helps swiftly uncover known and unknown threats



Benefits

- Focus on the right threats before damage is done
- Automate unique behavioral monitoring and response with risk scores to minimize alert fatigue and false positives
- Unify threat intelligence on a shared interface and storage platform for scalable and comprehensive coverage of known and unknown threats

Security teams are often faced with an overwhelming amount of alerts, many of which end up being false positives. These time-consuming, false leads make it difficult for analysts to effectively detect, triage, and respond to real threats within your enterprise in time.

When your analysts are overwhelmed and unable to spend their valuable time on real threats, you'll likely be left with a longer window of vulnerability for attacks and high-cost data breaches. On top of this, many tools are ineffective at detecting and responding to both known and unknown threats.

You need to focus your SOC on collecting and deriving valuable insights from massive amounts of threat intelligence to find threats, including insider and zero-day, before it's too late.

Preemptive threat detection

The OpenText SIEM product portfolio's automated, proactive, and holistic solution provides your SOC with layered analytics and contextual threat insights. With this, analysts can accurately prioritize threats and act swiftly to reduce potential impact.

Resources

Security operations

Learn more ›

Why the OpenText SIEM platform?

Our unique layered analytics approach helps SOCs efficiently detect and respond to known and unknown threats by seamlessly combining contextual threat intelligence derived from real-time correlation, behavioral analytics, and advanced threat hunting. Its intelligent use of machine learning helps minimize alert fatigue and false positives by identifying and prioritizing anomalous users and entities that may indicate an insider threat or advanced attack.

Combined with native SOAR by OpenText capabilities, these analytics work together to protect critical data and accelerate response. Your team can maintain comprehensive visibility while streamlining processes to speed action.

Features and benefits

- **Machine-learning powered threat prioritization**
  Reduce alert fatigue and focus on the threats that matter most. The OpenText SIEM platform combines supervised and unsupervised machine learning from OpenText™ Security Log Analytics to continuously identify anomalies, contextualize threats, prioritize leads, and reduce false positives across your environment.

- **Centralized user interface**
  Find and react to known and unknown threats quickly and accurately with a centralized user interface, which provides a holistic view of your entire threat landscape and reduces wasted time.

- **Security orchestration and automated response**
  Act quickly by automating repetitive tasks and initiating threat response with our SOAR capability.

- **Unique behavioral baselines**
  Detect hard-to-find, unknown threats such as insider, zero-day, and APTs, with additional threat context to reduce false positives and speed up detection time through accurate behavioral monitoring. The OpenText SIEM platform identifies unique baselines for all users and entities within your enterprise to uncover unusual and suspicious behaviors.

- **Custom risk scores**
  Work from a prioritized list of threat leads to identify suspicious users and entities and minimize alert fatigue based on customized risk scores derived from user and entity activity across your organization.

- **Holistic threat intelligence**
  Stop sifting through mountains of data to uncover threats. The OpenText SIEM platform combines threat intelligence with unified data storage and analysis to provide faster insights, boosting your SOC's detection and response times.

Copyright © 2026 Open Text • 09.26 | 241-000254-001

opentext™