Secureworks®

DATA SHEET

Secureworks® Threat Detection & Response

A Security Analytics application delivered on our cloud-native platform that improves threat detection and response across the entire ecosystem to drive better security outcomes.

Where Security Analytics Meets Threat Intelligence Expertise

With Threat Detection and Response (TDR) you can take security into your own hands and transform the way your security analysts detect, investigate, and respond to threats across your endpoints, network and cloud.

Built by security experts with over 20 years of security expertise TDR helps you to realize value fast with out-of-the-box security detection use cases that are continuously updated with threat intelligence from the Secureworks Counter Threat Unit™ (CTU™).

The combination of Security Analytics and Threat Intelligence expertise enables your security analysts to precisely pinpoint unknown and sophisticated threats with advanced analytics, accelerated investigation and response and community-applied intelligence.

Modern Threats Require Modernized Threat Intelligence

Threats are evolving. From the perimeter to the cloud, data travels in all directions, in unfathomable quantities, and at lightning speed. As a result, attacks have become more sophisticated and harder to detect. Couple that with limited visibility in the cloud, understaffed and under skilled security teams and the growing costs and complexity to manage disparate security systems and you can understand the importance for a modernized threat intelligence. As such, many SIEM detection use cases miss advanced threats and cause an influx of false positives resulting in wasted resources in responding to them. You're left struggling to build, apply and constantly update customized security content to your environment. All the while, threat actors are continuing to evolve their tactics, taking cover in the noise to act with stealth.

Secureworks Threat Detection and Response was built to solve these challenges. TDR's Threat Intelligence and Advanced Analytics-based Detectors are continuously updated to align with the current threat landscape.. You don't have to take any action to have relevant threat indicators loaded into the system or have stale indicators removed.

Why Secureworks' TDR

Advanced Analytics

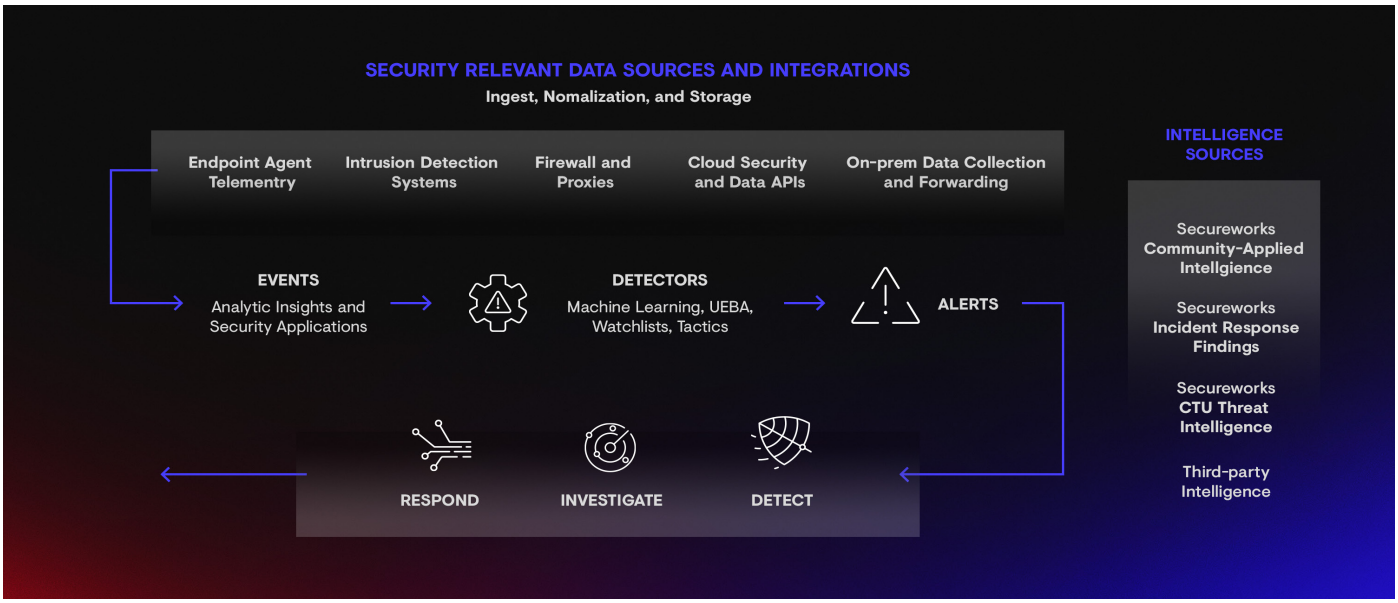
Protect against modern threats with machine learning, deep learning algorithms and UEBA

Accelerated Investigation & Response

Gain in-depth analysis of emerging threats to enable rapid response to attacks.

Community-Applied Intelligence

Share threat knowledge across our entire customer base to stay ahead of new attacks



Alert enrichment from Secureworks Threat Intelligence, entity context, geolocation, and other 3rd party enrichment data delivers in-depth analysis of threats, threat actor intent and behavior related to your alerts.

TDR delivers tangible value by enabling you to detect sophisticated threats, trust your alerts, streamline and collaborate on investigations and quickly respond with confidence.

Detect Sophisticated Threat

- Recognize adversaries by their behavior, be alerted to known and emerging threats in your environment, and quickly report to leadership if your organization has been hit in the past with an attack just discovered.

Trust your alerts

- Reduce the volume of threat alerts with minimized false positives from powerful and accurate analytics so your team sees only the recommended actionable insights that really matter.

Streamline and collaborate

- Empower your team to be more effective by removing silos so that they can knowledge share to speed up investigations and see full end-to-end attacker activity to paint a quick timeline of what unfolded. The “Ask an Expert” chat feature provides real-time collaboration with senior intrusion analysts.

Respond with Confidence

- Gain confidence that you’re taking the right action to contain a threat and let your security experts focus on security instead of mundane platform administration.

Key Differentiators

20+

Years of Attack & Threat Data

1400

IR Engagements Performed in the last year

300+

Expert Security Analysts, Researchers and Responders

52,000

Database of 52k unique threat indicators managed & updated daily

Transform SOC Efficiency and Efficacy

Secureworks' TDR enables your security operations teams to respond to security incidents with greater detection visibility. With capabilities such as extended log retention, search query, user-defined reporting and custom use case support, security analysts gain more ability to actively investigate and proactively hunt for threats in your environment. As a result, TDR can easily replace your current SIEM giving you advanced threat detection as well as additional SIEM capabilities to gain actionable insights into malicious activity. Our goal is to give you enough business and security context to make sense of an investigation and take the right action.

"Red Cloak™ TDR combines Secureworks' Red Cloak analytics with additional advanced tools previously unavailable to us. It's picked up threats we wouldn't have seen. Red Cloak TDR isn't just the next generation of SIEM, it's an evolution."

David Levine
Vice President Corporate & Information Security, CSO at Ricoh USA Inc.

Security Analytics with SIEM Capabilities

- Reliably ingest and retain events and raw logs across standard and custom data sources
- Quickly and easily search across data to enable rapid investigation and response
- Visualize data queries and share insights across the organization with flexible user-defined reporting
- Customize alerts to meet unique security use case requirements

TDR Benefits

- Retroactively identify suspicious activity in your environment as new IOCs emerge
- Speed up response and minimize damage with software-driven responses for common containment use cases
- Benefit from endpoint-based pricing that lets you send us your security relevant data without fear of hidden charges

About Secureworks
Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com