securonix

Four Ways to Unify Threat Detection, Investigation, and Response

Cybercriminals are more sophisticated, and the attack surface is constantly expanding. Demand for skilled cybersecurity professionals far exceeds supply. How can you defend against attacks across a wide-range of devices, networks, and applications and scale up resources to deal with these pressures? Moving to a unified threat detection, investigation, and response approach can help. Here are four areas to focus.

TRADITIONAL APPROACH

UNIFIED TDIR APPROACH

Siloed TDIR processes
Poorly integrated processes breed inefficiency and longer response time.

Simplified and streamlined TDIR
Establish TDIR as a continuum to remove fragmentation, reduce toil, minimize human error, and streamline incident response.

Disparate tools for TDIR
Too many technology pieces to operate and maintain. Too many moving parts, UIs, and lots of duplication.

Consolidated TDIR platform
Single UI reduces context switching. An embedded data cloud stores all security data in one place for consistent TDIR processes.

Compartmentalized defense
Time wasted searching for threat intelligence, indicators, and context. Lack of collaboration across teams and other organizations.

Proactive defense
Threat intel consumption across all phases of TDIR. Collaborate across teams and other organizations.

Insufficient detection content
Content is hard to produce and tune. The constant barrage of threats overwhelm organizations dealing with cyber skill and resource shortages.

Threat content-as-a-service
Continuously delivered threat intelligence and context. Stay ahead of new threats and improve your ability to detect and respond to incidents.

Ready to learn more about how to scale security operations to keep up with threat inflation?

DOWNLOAD THE WHITEPAPER

The Benefits of Unifying Threat Detection, Investigation and Response

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NDR, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo.

www.securonix.com

Follow us @securonix

securonix