SEQRITE

HawkHunt XDR

Extended Detection and Incident Response Solution

www.seqrite.com

Identify, track, and eliminate stealthy threats across all data sources through automated threat hunting and remediation.

Bring holistic protection to your enterprise across all attack vectors with SEQRITE HawkkHunt XDR.

Cyber threats are **getting smarter**. Is your enterprise equipped to defend them?

The year 2021 had witnessed a tremendous influx of advanced cyberattacks affecting nearly 47% and 27% of organizations (small, medium, and big) in the US and India, respectively. The trend continues in 2022, with high-profile breaches, such as at Red Cross and Microsoft, making headlines globally.

As per a study by SEQRITE's data scientists, the attacks are majorly categorized into two sections:

1. Evasive malware and Zero-day attacks
2. File-less attacks and targeted attacks

The latter two are the hardest to detect and the most destructive as they require historical analysis and correlation, along with machine learning techniques to be identified. Cyber security teams are aware of such targeted attacks but didn't have a simple yet powerful tool that could caution them by providing visibility across all data sources.

Basic Endpoint protection is insufficient to detect the most elusive malware and targeted attacks. Advanced detection and response mechanisms, strengthened with behaviour anomaly detection and historical events search, are necessary to combat them. In addition, you would need advanced automation mechanisms, as the volume of generated alerts can overwhelm the SOC team.

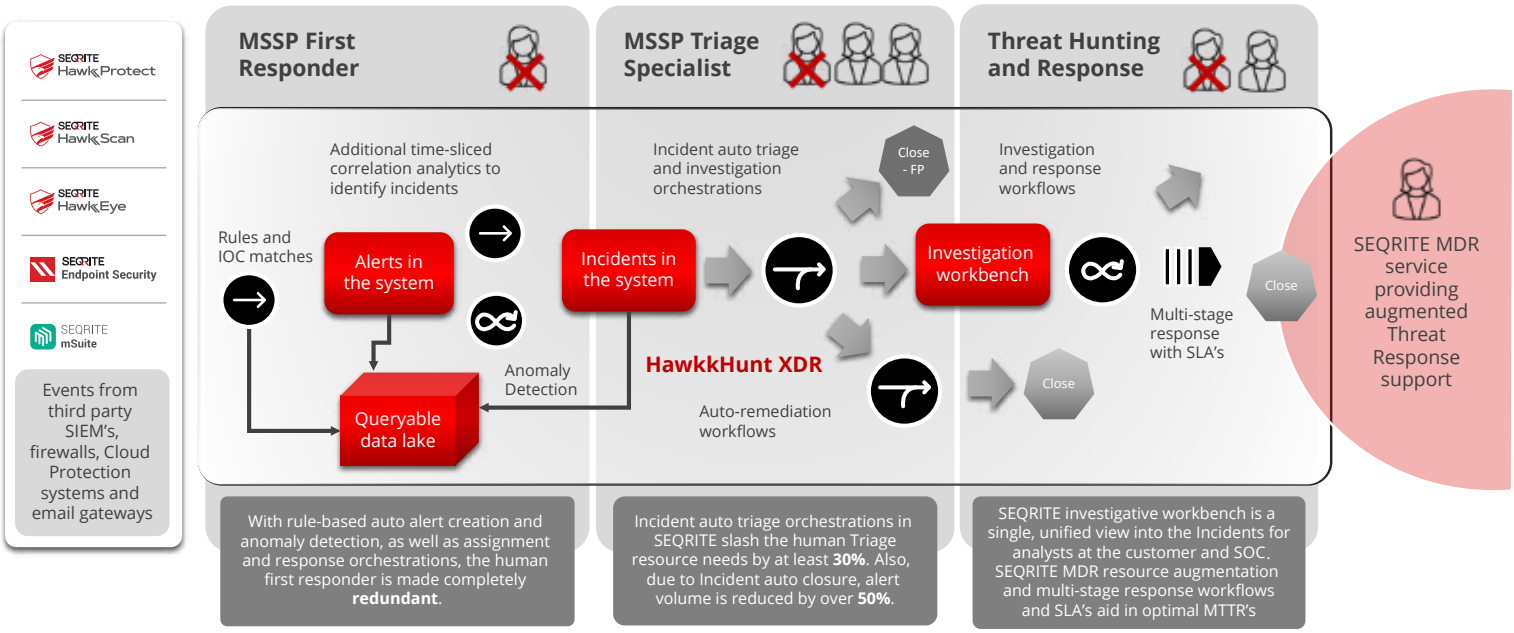
The Solution:
SEQRITE HawkkHunt XDR

An XDR Platform that enables a secure, hybrid SOC at a relatively lower price-point

SEQRITE HawkkHunt XDR is an advanced incident response tool that incorporates data from multiple security products into a unified security operations system to deliver holistic protection against cyberattacks. Using analytics and automation, SEQRITE HawkkHunt XDR centralizes, normalizes, and correlates data from various sources, thus enabling real-time cross-control-point protection while simplifying and strengthening the security processes.

SEQRITE HawkkHunt XDR blocks cyber threats by detecting malicious encryption processes and shuts them down before they disrupt any network.

How SEQRITE Hawkk platform enables the MSSP to perform Managed Detection and Response with 50% resource reduction



Product Highlights

Convenient: A single, holistic platform for Advanced Threat Detection and Response.

Precise: Throw fewer false positives due to focused source-specific logic.

Next-gen: Comes with enhanced properties like SOAR automation for Triage and Response, threat hunting workbench, IOC search and kill, and many more.

Multi-level protection: ML/AI for 24/7 awake vigilance. Behaviour Anomaly detection for additional protection against unknown threats. Automated Incident correlation and enrichment for severity assignment.

Response Management: Ensure optimal response times through Incident Management, SLA management, and detailed SOC Dashboards.

Playbook-based automation: SEQRITE HawkkHunt XDR ensures optimized resource utilization through automation.

Shared threat intelligence: The customer can source global threat intelligence and SEQRITE's in-house research-generated intelligence to tackle zero days and advanced persistent threats.

Historical data search: Historical data search allows IOC lookup for events that may have been missed earlier.

Support: SEQRITE MDR team available for response assistance and SOC resource augmentation.

Why Choose SEQRITE HawkkHunt XDR?

01 **Active vigilance**: Emphasis on Machine Learning, Behavior Anomaly Detection, automated IOC/IOA search, auto triggered remediation workflows for superior 24/7 active vigilance for the organization

02 **Years of expertise in cybersecurity**: With leadership in the endpoint security space for more than 20 years, 4 million+ endpoints secured, and an in-house research lab that provides up-to-the-minute IOCs and rules for locally and regionally active threat-actors.

03 **Focus on process orientation**: Tackling threats across the enterprise, across attack vectors and sources require single-minded process orientation. HawkkHunt XDR provides comprehensive incident management and SLA definition capabilities for procedure orientation of the SOC.

04 **Affordable price point**: SEQRITE has developed highly optimized storage algorithms that enable upto 180 days events and alert storage at a fraction of the cost of competitive offerings in the market.

Automation and ML for **24/7** lookout for APTs

Upto **180** days historical data search for missed IOCs

Incident and SLA Management at 50% resource reduction

About

SEQRITE is Quick Heal's Enterprise Security brand pioneering the future of cybersecurity with an autonomous and highly advanced range of enterprise security solutions. We are focused on simplifying the security stack and proactively safeguarding IT assets of businesses without forgoing enterprise capabilities. Our technology is designed to scale businesses and help secure the networks used by millions of customers globally. Are you ready?

SEQRITE

Quick Heal Technologies Limited
Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune - 411014, India.
Support Number: 1800-212-7377 | info@seqrite.com | www.seqrite.com