Seqrite **EDR Cloud**

SEQRITE

In the current era, stealthy cyber-attacks on enterprise endpoints have increased unprecedentedly. Traditional endpoint detection and response solutions are inadequate in such scenarios as they fail to effectively fetch the necessary data to detect and respond to unusual activities.

Seqrite EDR Cloud is a robust detection and response solution that solves this issue by providing customers with uninterrupted data visibility and greater control over their system hardware, Operating System, and applications. It allows customers to investigate past alerts and events, query the system for the latest information, and perform manual or real-time automated response and remediation.

Features of Seqrite EDR Cloud:

Multi-Phase Verification

Analyzes all system events via multiple layers of behavioral analysis, signature comparisons, and ML-based detection.

Immediate Host Isolation

Automatically or manually confines potentially infected hosts or take other automated actions, such as kill process, quarantine file, etc.

Automated and Manual IOC Lookup

Performs automated and manual IOC Lookups on historical data, sourcing IOCs from the latest Threat Intelligence data from the Seqrite Threat Intel team and other sources.

Advanced Notification Systemt

Integrates seamlessly with all SIEM solutions and sends SMS/email alerts.

Dashboard and Widgets

Presents a comprehensive system health overview, including top incidents, overall summary, affected incidents, and false positive rates via intuitive widgets.

Reports

Reports detail alerts summary over time, providing insights aligned with MITRE TTPs.

Rule Builder and Rules

Allows crafting system and custom rules. Leverages rule builder to craft personalized rules for capturing MITRE-related or other unusual or interesting activity on endpoints.

Action Policy Orchestration and Risk-Based Response

Implements real-time and offline response action policies, with defined scopes for risk-based auto-response using generic or custom policies.

Investigative Workbench

Helps investigate incidents and alerts with detailed drill-downs, contextual information, query-based access to live system information, and thorough listing of alerts access to alerts list and alerted tree, enabling centralized alert actions from one location.

Incident Management

Enables incident management through the incident list and information on endpoints and users while formulating remediation actions.

SEQRITE
AVOSEC
Software Distribution

Benefits of Seqrite EDR Cloud

Deter advanced attacks

Our Endpoint detection system analyzes each telemetry event generated at the sensors through multiple analysis stages to perform a thorough contextual analysis. If suspicious activity is detected, our EDR system can immediately block it.

Stop Malware before it strikes

By taking automated real-time actions, like isolating the system or stopping the execution, an adversary's chances of executing a successful attack are greatly diminished.

Benefit from thorough investigations By compiling highly useful information regarding executions, scripts, commands, and process chains, the security analysts' time for triage and response is significantly reduced. This feature expands the capability to meet compliance needs and standards.

Reduce the need to hire outside Incident Response and Forensics Firms

Our Endpoint Detection & Response module allows the security analyst and IT administration teams to conduct detailed investigations of attacks independently, reducing the need to engage external agencies to conduct such investigations.

Look up Historical data for hidden threats

Advanced attacks use stealth technology to remain hidden in the environment for many months. Utilizing our event data storage and Threat Hunting, combined with the latest Threat Intelligence, such hidden threats can be discovered, and immediate response actions can be taken.