DTS

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

SECURITY INFORMATION & EVENT MANAGEMENT

Many companies still only use reactive mechanisms to protect themselves against cyberattacks. However, these conventional measures can usually only limit the damage. The best chance of defense in the area of cybersecurity is the early detection of potential threats. Security Information and Event Management (SIEM) is a great preventative approach. LogRhythm's impressive security intelligence platform, a leader in the Gartner SIEM Magic Quadrant, detects anomalies in real time, with the ability to take immediate countermeasures and defend against serious threats. As a LogRhythm Services Authorized Partner, we enable this solution and thus proactive cyber protection, especially in conjunction with our DTS Security Operations Center (SOC) as a complete, central security control center.

- End-to-end transparency of the IT environment in real time
- Multi-dimensional identification of anomalies in user, host & network behavior
- Independent monitoring of forensic data & file integrity
- State-of-the-art hardware analysis & analysis of large datasets
- Intelligent correlation & pattern recognition
- Minimal detection & response time
- Scalable approach & workflow-enabled automation
- DTS managed services
- DTS SOC services

Conventional SIEM solutions include the right preventive approach. However, they are not able to keep up with the requirements of modern cybersecurity. They only collect and analyze data from security events, require a lot of administration due to a lack of automation and make it difficult to expand for additional use cases. They also contribute little to the selection of alerts and orchestration, which promotes alert fatigue and uncertainty.

Protection against modern threat scenarios requires end-to-end transparency of the entire IT environment. In addition, speed and precision are required in an emergency. LogRhythms SIEM combines log management, file integrity monitoring and hardware analysis, monitoring and artificial intelligence with forensic host and network data in a fully integrated platform. The global overview of all activities enables the detection of anomalies that would otherwise go unnoticed. The greatly reduced detection and response time for anomalies and threats differs significantly from conventional solutions.

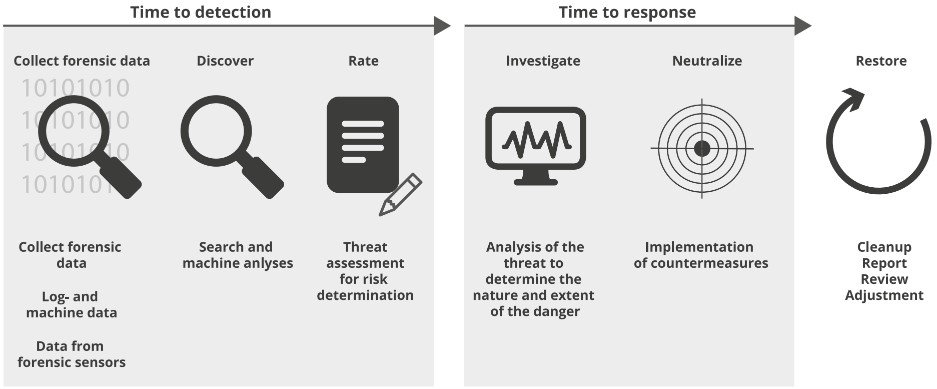
The architecture of the LogRhythm XDR stack offers a standardized solution that adapts flexibly and scalably to the individual needs of the corporate environment. With the help of the Log Management & Analytics, Security Analytics & Security Orchestration, Automation & Response (SOAR) modules, threats are fully detected and responded to appropriately.

LOGRHYTHM ANALYTIX helps you diagnose safety and operational issues by providing centralized and comprehensive visibility into your entire data inventory. AnalytiX streamlines the collection and access of critical log and other machine data. It normalizes and enriches your data so that search and analysis can be performed quickly, regardless of how and where the data was generated.

LOGRHYTHM DETECTX provides customizable security analytics that can accurately detect malicious activity and actively support threat hunting. By correlating the data, the security analysis detects such actions to generate prioritized, risk-based alerts.

LOGRHYTHM RESPONDX simplifies threat investigation and response by coordinating and automating as many steps as possible in the response process. It establishes consistent processes that help our DTS Security Operations Center (SOC) team organize, prioritize and collaborate to achieve maximum efficiency and speed.

The LogRhythm SIEM offers a unique threat lifecycle management approach. By integrating essential functions into one platform, the XDR stack not only provides you with a cost-efficient SIEM, but also enables immediate detection of threats.


Time to detection
Time to response
Collect forensic data
Discover
Rate
Investigate
Neutralize
Restore
10101010
Collect forensic data
Log- and machine data
Data from forensic sensors
Search and machine anlyses
Threat assessment for risk determination
Analysis of the threat to determine the nature and extent of the danger
Implementation of countermeasures
Cleanup
Report
Review
Adjustment

DTS MANAGED SERVICES & SOC SERVICES

DTS specializes in the design, implementation and operation of LogRhythm SIEM. We bundle this technology for our customers with our expertise and processes to enable dedicated SIEMaaS and SOCaaS models. On this basis, we not only offer you an increased level of cybersecurity, but also save costs, time and human resources.

Our DTS SOC is a major advancement in cybersecurity, especially when combined with LogRhythm's state-of-the-art SIEM. It is a central security control center for 24/7 monitoring and support of your IT infrastructure and data. Among other things, we use the LogRhythm SIEM to ensure end-to-end visibility, analyze specific IT resources and data almost in real time, detect the anomalies mentioned, issue alerts and defensive recommendations and constantly derive new rules for effective defense. Our highly qualified, experienced, experienced, German and English-speaking security experts guarantee around-the-clock: managed security services, active monitoring & analysis of your IT systems, detection and removal of IT vulnerabilities, central security management, alerting & defensive measures, security assessments, event and log management, compliance and reporting.