# DTS

## Security Information and Event Management (SIEM)

## Security Information and Event Management

*Many companies still use only reactive mechanisms to protect themselves against cyber attacks. However, these conventional measures can usually only limit the damage. In the field of cyber security, the best chance of defense lies in the early detection of potential threats. Security Information and Event Management (SIEM) is a great prevention approach in this context. 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 avert serious threats. As a LogRhythm Services Authorized Partner, we deliver this solution for you, providing proactive cyber protection.*

- Continuous 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
- Minimum detection & response time
- Scalable approach & workflow-enabled automation
- Optional DTS SOC services

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

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

The LogRhythm XDR Stack architecture provides a unified solution that is flexible and scalable to meet the unique 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 or an appropriate response is triggered.

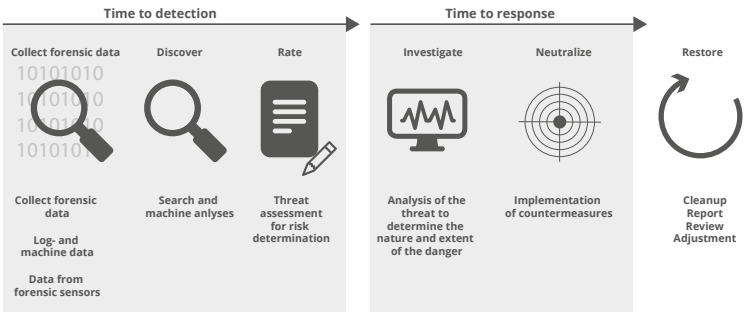
**LogRhythm AnalytiX** helps you diagnose security and operational issues by providing centralized and comprehensive transparency across your data. AnalytiX optimizes collection and access to critical log and other machine data. It normalizes and enriches your data so that search and analysis can be performed quickly, regardless of how and where the data was generated.

**LogRhythm DetectX** delivers customizable security analytics that can accurately detect malicious activity and actively support threat hunting. By correlating the data, security analytics 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 in one platform, the XDR stack not only provides you with a cost-effective SIEM, but also with immediate threat detection.

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






**DTS Systeme GmbH**
+49 5221 1013-000

**DTS Systeme Münster GmbH**
+49 251 6060-0

**DTS Systeme Wien GmbH**
+49 5221 1013-000

**www.dts.de**
info@dts.de