Managed SIEMaaS

(SIEM as a Service)

As compliance requirements continue to expand and the demand for advanced threat detection increases, organizations need to deploy a Security Incident and Event Management (SIEM) solution. However, they often find that it's both costly to implement and resource intensive to maintain. In addition to the large capital outlay; finding and hiring experienced security experts to manage the platform 24X7X365 can be difficult and incur high operational costs.

Thrive's Managed SIEM as a Service (SIEMaaS) offers our clients a fully managed, hosted SIEM solution which provides a service-oriented IT infrastructure monitoring platform. The system collects data from hosts, network devices, applications, and security platforms within the organization, and adds real-time context analytics, and alerts for a more complete understanding of the environment.

Thrive's Managed SIEMaaS provides each customer with dozens of pre-configured and customizable reports that provide insight into compliance, performance, availability, and security across every discipline of IT.

Thrive Managed SIEMaaS Includes:

- Data Collection Discovery
- Bi-WeeklyThrive Security Team Reviews
- Ongoing Assistance with Device Discovery and Alert Optimization
- Creation of Report Bundles
- Creation of Customer Dashboards
- Customized Remediation Services

Built upon the robust Fortinet FortiSIEM platform, Thrive Managed SIEMaaS provides advanced correlation of internal log data with threat intelligence feeds provided through FortiGuard Labs, which consists of hundreds of research specialists, with over 16 years' experience in threat research and response, providing cutting-edge protection to customers and enhancing their cybersecurity defense.

- Real-Time, Automated Infrastructure Discovery and Application Discovery Engine (CMDB)
- User and Entity Behavior Analysis
- Cross Correlation of SOC & NOC Analytics
- Out-of-the-Box Compliance Reports
- Self-learning baselines
- Real Time Analysis of Security & Network Threats