

OPTICS FOR SECURITY

SECURITY INFORMATION MANAGEMENT

Once you've experienced a security breach or operational issue, how quickly can you search your log files, identify the source, and remediate?

Are you able to use the data in your log files to proactively mitigate risk in your environment?

Are you managing your log data to comply with regulatory requirements?

Optics for Security Information Management (Optics for SIM) is a GlassHouse security service offering for log management and security reporting that provides greater visibility into your security posture, improves operational efficiency, and enables successful compliance audits by turning IT data into actionable business information.



Optics for SIM:

- Collects and centralizes log data
- Indexes log data and provides for simplified searching
- Normalizes and tags data for advanced correlation and analytics
- Includes pre-defined alerts and reporting
- Allows for customized views and reports
- Presents security views and dashboards via an intuitive web portal interface
- Provides industry-based compliance reporting and audit trails

Optics for SIM enables advanced security reporting, correlations, and incident handling to help detect, respond, and prevent security related issues. Out of the box security views include:



- Access Control
- Endpoint Protection
- Network Protection
- Governance
- Audit and Data Protection
- Incident Response and Management



Optics for SIM manages log data:

- Centralize
- Normalize
- Analyze
- Interpret
- Alert
- Report
- Retain

According to the results of a SANS Institute survey:

"The one thread that shows up numerous places throughout this survey is a need for simpler processes of mining logs for valuable data that could point to weaknesses, intrusions, violations and inefficiencies that need attention and repair. This is difficult to achieve because there is little consistency among firewalls, IDS, routers and switches, operating systems, databases, production applications and myriad other devices that produce and store log data."

OPTICS FOR SECURITY

SECURITY INFORMATION MANAGEMENT

The service includes:

Log Management

- **Data Collection** – collection capabilities for virtually all available IT data types including SNMP, Syslog, database, file, scripted inputs, and more.
- **Data Indexing** – the collected data is centralized, parsed and indexed to allow for “google-like” search capabilities.
- **Data Retention** – the data is retained as per the customer requirements based on specified internal policy or dictated by regulatory compliance. The data can be retained and may also be stored offline for longer term archiving.

Proprietary Framework

- **Data Analytics** – the data is parsed, normalized, and interpreted to pull out events of interest.
- **Data Correlation** – the framework allows meaningful correlation and analysis across disparate technologies including Cisco, Juniper and Checkpoint, Symantec and McAfee, Linux and Microsoft, and more.
- **Flexible** – the framework can be applied to any third party solution within your environment and can even be utilized to integrate log data from custom applications.

Security Intelligence

- **Security Views** - Integrated security dashboards, searches, analysis, reports and alerts.
- **Web Interface** – the data is accessible via a secure web interface that can be used for searches, viewing reports, and managing the solution.
- **Reporting** – the data is summarized based on customizable event criteria and can be viewed interactively via the web interface.
- **Alerting** - when data matches selected event criteria it becomes an “event of interest”. When data becomes an “event of interest” the customer is alerted and appropriate action can be taken.



GlassHouse Technologies is a global provider of data center infrastructure consulting services. Focused on data center consolidations, virtualization, security, storage, data protection and managed services, GlassHouse consultants offer a vendor-independent approach to architect, implement and operate IT environments that drive high performance and agility through cloud computing and a service provider model. GlassHouse transforms infrastructures to deliver high value services that align to business needs, enabling cloud computing and accelerated return on investments while mitigating operational inefficiencies and risk. This is provided through Transom, a unique delivery framework comprised of proprietary software tools, methodologies and domain expertise. Visit the GlassHouse blog for expert commentary on key data center issues facing today's enterprises and follow us on twitter at #GlassHouse_Tech.