

Security Monitoring

"All Eyes on Glass Security Monitoring"

Collection & analysis of security events, as well as a wide variety of other contextual data sources



Real Time Monitoring



Forensic Investigation of Incidents and Events



Risk Assessment



Reporting



Customer Access to Incidents and Alerts with Live Chat



Automated Event Response



Event Discovery & Prioritization

Requirements

- ✓ Alert triage
- ✓ Incident validation
- ✓ Recommended remediation
- ✓ 24/7 coverage

Benefit

- ✓ Vendor agnostic
- ✓ Custom dashboards and reports
- ✓ Live chat

Use Cases

- ✓ SOC as a service
- ✓ Managed Detection and Response
- ✓ Managed Threat Detection
- ✓ Breach Response

Solutions

- ✓ Multi-vendor log aggregation
- ✓ Alert correlation & analytics
- ✓ Incident validation and notification
- ✓ Threat hunting
- ✓ Human factor

Evolution

- ✓ 360 SOC GUI
- ✓ War Rooms & Unprecedented Incident Collaboration
- ✓ 100% Technology Agnostic "Open" Platform

360 SOC