LOOKINGGLASS

ScoutVision

THREAT INTELLIGENCE MANAGEMENT

Transforming the Art of Threat Intelligence

ONE SYSTEM: THREE BENEFITS

SCOUTVISION™ Threat Triple Play (TTP) is an effective counter to the tactics, techniques, and procedures (TTP) malicious actors use to breach your networks.

1

Threat Intelligence Analysis

- Multi-source, Internet intelligence based attack surface visibility
- Configurable TIC scoring delivers industry and organizational relevance
- Connect your security infrastructure to threat intelligence with simple to use API's

2

Incident Response

- Correlation of network telemetry and threat intelligence to prioritize security events
- Ad hoc and scheduled reports enable insight for security stakeholders

3

Third-Party Risk Monitoring

- Dynamic risk mitigation with proactive and continuous monitoring of CIKR sectors, ecosystem partners and your supply chain
- Dramatic risk reduction with 360° view including peer relationships, M&A targets, alliances, and vendor relationships

Effective risk decisions depend on analysts harnessing multi-source threat intelligence and understanding when and where threats intersect the Internet, the enterprise, and their 3rd party ecosystem. LookingGlass™ ScoutVision™ provides comprehensive and relevant risk information, streamlines work flows, delivers analysis and threat confidence, and dramatically increases productivity. ScoutVision combines continuously updated Internet intelligence with hundreds of correlated threat intelligence data feeds and summarizes in a powerful yet intuitive sharable workspace—enabling threat analysts to deliver both strategic and tactical guidance to their stakeholders.

Enriched Threat Intelligence

Threat intelligence analysts and big data analytic systems strive to discover and understand relationships and patterns among multiple indicators that are buried by the sheer volume and diversity of threat data. Finding the signal in the noise requires a challenging integration of big data analytics and threat research analysis, the combination of which are rare in the cyber threat intelligence community. Many vendors offer 'intelligence' that is essentially a narrow set of indicators confined to a specific incident or a handful of elements. Multiple vendors use different terms to describe the same incident and indicators. Only LookingGlass combines decades of threat research expertise with correlated, multi-source threat and Internet intelligence and a big data architecture to enable rapid analysis and mitigation of existing and emerging threats.

The ScoutVision foundation is a continuously updated cyber threat map—a real-time representation of the Internet's infrastructure, connectivity, and asset ownership combined with threat observations including malware, TTPs and actors. Only LookingGlass ScoutVision delivers true Internet intelligence on global IP and DNS registrations, autonomous systems, and routing activity. ScoutVision then aggregates our proprietary threat intelligence, including the world's largest bot-net sensor network, and fuses it with hundreds of threat data feeds from open source and commercial providers. The result is a comprehensive threat intelligence management system, complete with API's and applications for integrating with other security platforms, including internal network and threat telemetry. ScoutVision provides unmatched context for understanding cyber threats and risks—revealing spatial, temporal, ownership, and indicator relationships both historically and in near real-time.

KEY FEATURES AND BENEFITS

Breadth and Quality of Aggregated Threat Data

ScoutVision combines open, best-of-breed commercial, community, and organization derived intelligence sources with our own global array of sensors and data feeds that offer active probing and measurement, passive data gathering, malware analysis, and intrusion monitoring. The result is early detection and warning of Internet threats.

Internet Intelligence

The LookingGlass Global Internet MonitoRing (GLIMR) network collects results from tens of millions of network topology probes daily. Internet routing events and network path discovery form an accurate Internet topology map. GLIMR implements several mechanisms to enumerate Internet hosts seen as threat risks. Deep Internet intelligence provides the necessary foundation to apply context to threats leading to better risk management.

Threat Indicator Confidence

Only ScoutVision enables threat analysts and security operations teams to customize the aggregation of millions of threat indicators into a universal Threat Indicator Confidence (TIC) score that is normalized and tunable to match the security posture and risk profile of their organization. ScoutVision Threat Indicator Confidence provides a completely transparent, out-of-the-box threat confidence score while allowing users to customize the weight and priority of indicators based on their environment, threat landscape and organizational imperatives.

Multiple Deployment Configurations

ScoutVision can be hosted on behalf of the customer at LookingGlass' secure data center or deployed on the customer premises.

Comprehensive Sharing and Collaboration

Within an organization, ScoutVision provides a broad range of secure collaboration options, including both individual and group sharing across investigation projects. ScoutVision also provides standards-based export and import of threat data to share across organizations.

Scalability and Flexibility

The ScoutVision architecture scales with a private cloud based core intelligence processor (CIP) managing all feed and Internet intelligence data. The CIP delivers to customer-facing processors all data to which customers subscribe. The bidirectional Cloud – Customer model enables broad scalability.

Visual Search and Pivot Big Data Operations

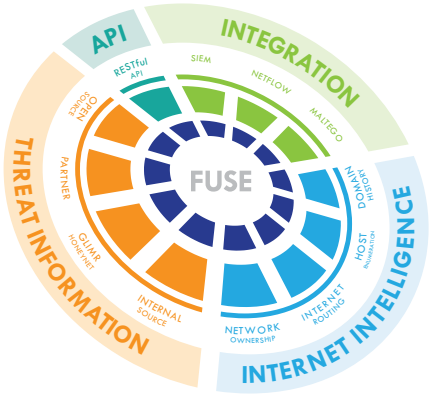
ScoutVision performs the big data operations of extract, transform, and load for all ingested feeds and gives analysts the ability to explore relationships through an interactive graph. ScoutVision is based on a high performance key-value database operating on a high-availability, low-latency, hyper-converged infrastructure (HCI) hardware platform.

Extensible API

ScoutVision includes a RESTful API enabling customers to integrate with other security analytics tools.

Optional Network Telemetry

LookingGlass ScoutInterXect accelerates and optimizes security incident response. Integrated with ScoutVision, ScoutInterXect delivers network telemetry correlated with context-specific threats to zero in on specific network hosts interacting with internet threats.



LookingGlass' innovative threat intelligence management system delivers content, context, and confidence in risk and security operations decision support. LookingGlass increases visibility within and beyond the network perimeter, empowering customers to continuously assess and mitigate threats.

LookingGlass Cyber Solutions, the leader in threat intelligence and dynamic threat defense, enhances security operations through verified multi-source threat information fused with real-time Internet intelligence. LookingGlass delivers threat intelligence analysis, management, and mitigation systems that empower customers with comprehensive risk insights to confidently enable effective security decisions and efficient security operations.

For more information, visit **www.lgscout.com**
or call **888.SCOUT.93**