DEFENSESTORM
THE BEST OFFENSE.

GRID Active Threat Surveillance

Get ahead of threats with the built for banking cyber risk management solution

Financial institutions like yours need to have full visibility of the threats they are up against, the ability to make informed actions, and protect against those threats. DefenseStorm is the only cybersecurity solution built for banking that consolidates cybersecurity data for real-time visibility into your security operations and threat detection, reducing false positives so you can prioritize and act on the most severe threats.

As a financial institution, you're in a state of constant operational change expanded digital offerings, upgraded technology at existing branches, opening new branches, and adding new employees are all reasons to celebrate change, but they also open the door to cyber risk.

GRID Active Threat Surveillance gathers and analyzes data from all types of sources, technology, tools, and systems and identifies threats in your environment. This unique built for banking approach to security leverages our GRID Active intelligent data platform that integrates cyber risk management solutions which are enabled and enhanced through machine learning to monitor the network proactively and continuously for known attacks and suspicious activity.

With GRID Active Threat Surveillance security data is consolidated from across your organization for real-time visibility and threat detection to support a solid cyber risk management program.

FEATURES

- Cybersecurity protection that is inclusive of unique technology and requirements for financial institutions.
- Ability to add EDR functionality integrated to GRID Active
- Integration with GRID Active, our cloud-based intelligent data platform that integrates cyber risk management solutions.

BENEFITS

- Allows ingestion of data across the unique technology to enhance protection and maintain requirements for financial institutions.
- Protect cloud, perimeter, network, endpoints, applications and data against
- cyberattacks.
- Integrated cyber risk management platform that is enabled and enhanced through machine learning.

By creating a program that includes threat detection, reducing false positives, and prioritizing events you can focus on the threats that matter most. In support of your cyber risk management program, GRID Active Threat Surveillance gives you the ability to regularly review your environment and apply corrective actions by verifying that threats have been eliminated. You also have access to our team of experts who are with you every step of the way from implementation and product training to platform support to ensure you remain cyber risk ready.

DEFENSESTORM
THE BEST OFFENSE.

GRID Active Threat Surveillance

- Full visibility, transparency and access to alert statuses, event and logs to better manage overall cyber risk readiness.
- GRID Active configuration logs are fully visible to allow customers to see how your unique environment is monitored.
- Insights and updates from our cyber threat intelligence (CTI) team to defend against new threats across the FI.
- Ability to monitor data across the unique and complex technology systems of financial institutions.
- Available Vulnerability Management Services for continuous risk mitigation and posture improvement with integrated reports through the GRID Active platform
- Use of Machine Learning and AI to better defend against threat actors and decrease time to detection.

PatternScout: Provides better detection of anomalies that may be evidence of suspicious or malicious behavior in the network that would not be detected through a rules-based system.
ThreatMatch: Automatically aggregates threat intelligence feeds to find known bad actors (IP, domain name, file hash) that could be affecting your network now or in the past
Incident Similarity: An AI model that compares two incidents' (IP addresses, text, devices or application names, countries of origin, API keys, hostnames) and associated events. By elevating the view and providing a comprehensive view of a financial institution's (FI) incident monitoring requirements, FIS gain additional insight into security concerns across their organization and enhance their incident management.

Access to Managed Services

With GRID Active Threat Surveillance you have access to Cyber Threat Surveillance Operations (CTS Ops) team of analysts and engineers who continuously monitor and can protect your network when you need it, either 24/7 or with After-Hours support. The team is comprised of certified cyber professionals to augment an FI's staff and investigate alerts on their behalf, allowing them to focus on their core business.