PRODUCT SOLUTION

DEFENSESTORM
THE BEST OFFENSE

Managed Detection & Response Built for Banking

Always-on threat detection, expert-led investigation, and guided response, purpose-built for the security and oversight needs of banks and credit unions.

THE CHALLENGE

Rising Threats, Lean Teams, and Generic Tools That Weren't Built for Banking

Cyber threats targeting financial institutions are growing in volume, speed, and sophistication, yet most FIs lack the staffing and specialized tooling to operate a 24x7 security operation. The result is fragmented visibility, alert fatigue, slow investigations, and mounting pressure from examiners and boards demanding stronger evidence of program effectiveness.

Generic MSSP and MDR providers add another layer of complexity: tools that weren't built for banking, analysts unfamiliar with examiner expectations, and reporting that doesn't map to FFIEC, GLBA, or NCUA frameworks.

THE SOLUTION

DefenseStorm MDR: Detection and Response, Reimagined for Banking

DefenseStorm MDR unifies SIEM analytics, 24x7 SOC monitoring, and integrated endpoint detection into a single, fully managed service, purpose-built for banks and credit unions.

Our SOC analysts don't just monitor dashboards. They investigate with full banking context, triage with precision, and guide your team through response, acting as a true extension of your staff while delivering the oversight evidence examiners expect.

ONE SERVICE. THREE PILLARS.

Complete Detection & Response Coverage

DefenseStorm MDR integrates three critical capabilities into a single, fully managed service, powered by the GRID Active platform and backed by our Collaborative SOC.

Threat Surveillance (SIEM)

Real-time log ingestion, correlation, and AI-driven behavioral analytics across your entire technology stack, with detections tuned for financial services and auto-mapped to FFIEC, GLBA, and NIST.

24x7 Security Operations (SOC)

Around-the-clock monitoring, triage, investigation, and guided response from certified analysts who work as a collaborative extension of your team with full banking context.

Integrated Endpoint Detection (EDR)

Your chosen EDR solution (CrowdStrike, Microsoft Defender, Carbon Black) integrated directly into MDR workflows. No rip-and-replace, no separate tool management.

WHAT MDR DELIVERS

Outcomes That Move the Needle

Faster Detection, Smarter Triage

AI-driven behavioral analytics reduce noise and surface confirmed threats faster. SOC analysts acknowledge alerts in 82 seconds (MTTA), with enriched context and dynamic risk scoring that eliminates false-positive fatigue.

Key outcome: Your team focuses on real threats, not noise.

Continuous Coverage Without Building a SOC

24x7 monitoring, investigation, and guided response from certified analysts who understand banking, delivered as a collaborative extension of your team. No hiring, no training, no coverage gaps.

Key outcome: Full SOC coverage at a fraction of the in-house cost.

Examiner-Ready from Day One

Every detection is automatically mapped to FFIEC, GLBA, and NIST controls. Continuous oversight reporting gives your CISO and board exam-ready evidence of program effectiveness without manual evidence collection.

Key outcome: Walk into any exam with confidence.

One Platform, Complete Visibility

SIEM, SOC, and EDR unified in one service powered by GRID Active. One vendor, one platform, one pane of glass for detection, investigation, and response.

Key outcome: Fewer vendors, less complexity, clearer oversight.

Your Collaborative Security Operations Center

DefenseStorm's Collaborative SOC is comprised of certified cyber professionals who act as a true extension of your staff. Available 24x7, they triage alerts, investigate threats, and guide response, all within the context of banking oversight and examiner expectations.

This is not an outsourced service. It's a collaborative partnership built to augment your existing team, allowing you to focus on your core business while maintaining the coverage examiners expect.

Why DefenseStorm

Built for Banking
The only MDR service designed exclusively for banks and credit unions, with detections, workflows, and reporting aligned to FFIEC, GLBA, and NCUA expectations.

Unified MDR Platform
SIEM + SOC + EDR in one integrated service. Fewer vendors, less complexity, and a single pane of glass for detection, investigation, and response.

Collaborative SOC
CTS Ops analysts available 24x7 as a true extension of your team: banking-focused triage, investigation, and guided response with clear visibility and defined escalations.

EDR Choice
Integrate your preferred endpoint solution (CrowdStrike, Microsoft Defender, Carbon Black) directly into MDR workflows. No rip-and-replace required.

Examiner-Ready Evidence
Continuous oversight reporting with detections automatically mapped to regulatory controls across FFIEC, GLBA, and NIST frameworks.

By the Numbers

82 sec Mean Time to Acknowledge (MTTA)	**<15 min** MTTD: critical alerts	**<40 min** MTTD: all severities
<24 hr MTTR for critical incidents	**95%+** SLA compliance on triage and response	**~7,000** Critical alerts triaged daily from 5M+ events
92% MITRE ATT&CK techniques actively covered	**5M+** Events ingested and analyzed daily	**200+** Banks and credit unions protected

When it comes to managed detection and response, **DefenseStorm is the best offense.**
See how DefenseStorm MDR can extend your team with 24x7 detection and response built for your institution.

470-519-0020
info@defensestorm.com