PRODUCT DATA SHEET · MANAGED DETECTION & RESPONSE

CATCH REAL THREATS FASTER, AND STOP CHASING THE NOISE

DefenseStorm MDR brings SIEM, a 24x7 Collaborative SOC, and EDR into one service, built only for banks and credit unions. Banking-fluent cybersecurity analysts watch your environment around the clock, so your team works real threats instead of false positives.

THE CHALLENGE

Your environment generates millions of events a day. Prior providers were slow and reactive, teams drown in false positives, and boards and examiners demand stronger proof that the program works. Lean teams cannot staff a 24x7 SOC on their own.

THE SOLUTION

One service: SIEM, a 24x7 US-based Collaborative SOC, and EDR, built only for banks and credit unions. Automation does the legwork across 750+ detection triggers, and a senior analyst owns the decision. It works as an extension of your team, not a black box.

KEY CAPABILITIES

- **Unified SIEM and EDR visibility.** Bring logs and endpoint activity into one platform for a single view of your environment.
- **Response on the EDR you already run.** Our Collaborative SOC monitors, triages, and responds across CrowdStrike, Carbon Black, and Microsoft Defender. Automated response is live today, scoped to high-confidence critical detections, least-privilege, fully logged, and reversible. No rip-and-replace.
- **A 24x7 Collaborative SOC.** Banking-fluent cybersecurity analysts triage, investigate, and guide response. A senior analyst on every case, no Tier 1 queue, no bot.
- **Examiner-ready evidence as a byproduct.** Detections are built from real banking attacks, and every investigation maps to the frameworks and exam procedures that apply to your program.

FROM MILLIONS OF EVENTS TO A HANDFUL OF REAL CASES

01
Unify your data.
Logs and endpoint activity in one platform.

02
Cut the noise.
Automation enriches and correlates across 750+ detection triggers, so real threats surface and false positives fall away.

03
A senior analyst takes the case.
Investigated with context, within minutes, 24x7x365.

04
Respond with judgment, not just speed.
Automation handles volume; the analyst owns the response.

05
Prove it.
Every investigation becomes examiner-ready evidence, mapped to your frameworks.

KEY BENEFITS & OUTCOMES

- **Noise cut, signals surfaced.** Prioritized, enriched alerts end alert fatigue, so your team works a handful of real cases instead of a wall of false positives.
- **Extend your team without new headcount.** A senior analyst guides response around the clock, so lean teams get always-on coverage without hiring.
- **Proof for boards and examiners.** Continuous evidence mapped to NIST CSF 2.0, the CRI Profile, and the exam procedures that apply to your program, generated as a byproduct of monitoring.
- **Detection and response in minutes.** Unified SIEM and EDR visibility with 24x7 Collaborative SOC triage means real threats surface and get owned fast.
- **Protect the investments you already made.** We monitor, triage, and respond on the EDR you already run, so you consolidate without a rip-and-replace project.

BUILT FOR THE TEAM THAT OWNS SECURITY

For the CISO or ISO.
Get 24x7 coverage without adding headcount, and a program you can prove to your board and examiners. Escalations arrive in language they understand, and every investigation becomes evidence automatically.

For the security and IT team.
Fewer false positives, tuning that sticks, and a senior analyst on the line when it counts, so you spend your week on real priorities.

For the CTO or CIO.
Consolidate SIEM, SOC, and EDR into one predictable, banking-specific service that integrates with the core and the EDR you already run, with no rip-and-replace.

BY THE NUMBERS

~80M → 3 events a day per institution filtered to the few that need a person (99.9% noise reduction)	**< 3 min** typical detection (MTTD), from data reaching us to a tracked investigation	**~5 min** to a named analyst claiming the case (MTTA)
< 20 min client notification, under 8 minutes for critical	**98%+** of tested attacks detected (independent pen testing, trailing 365 days)	**750+** detection triggers, fully viewable
200+ banks and credit unions	**~$170K** saved a year from tool consolidation	**Built for Banking** banks and credit unions only, since day one

STOP CHASING ALERTS. START HANDLING THREATS.

See what a banking-only MDR service looks like inside your environment, with a senior analyst on every case.

TALK TO A SPECIALIST | GET A DEMO

470-519-0020 | info@defensestorm.com | defensestorm.com