PRODUCT DATA SHEET · COLLABORATIVE SOC

AROUND-THE-CLOCK THREAT COVERAGE, WITHOUT GROWING YOUR TEAM

A 24x7 team of cybersecurity analysts, fluent in banking, monitors, investigates, and guides response as an extension of your team, so a real analyst has the watch even at 2 a.m., and every escalation comes in language your examiner understands.

THE CHALLENGE

Most managed SOCs were built for enterprises that look nothing like a community bank, staffed by analysts who have never answered to an examiner or reported to a credit union board. Under roughly $1B in assets, examiners expect a managed service, not in-house staffing.

THE SOLUTION

The opposite: banking-only, transparent, and senior. A Collaborative SOC monitors and investigates as an extension of your team, not a fully outsourced black box. You keep control of the decisions that are yours, and we own the around-the-clock work you do not have the hours for.

THREE CAPABILITIES THAT WORK AS ONE

A senior analyst on every case.

When you contact the SOC, you reach a senior cybersecurity analyst, fluent in the challenges unique to banking, 24x7x365. No Tier 1 queue, no bot.

Detections built from real banking attacks.

Because we monitor banks and credit unions exclusively, an attack on one institution becomes protection for all of them. Financial-sector threat intelligence from real attacks gives the team early indicators used to protect every institution we monitor.

Protection that reaches the endpoint.

We extend monitoring and response to the endpoint, on the EDR you already run. Our Collaborative SOC monitors, triages, and contains on your behalf across CrowdStrike, Carbon Black, and Microsoft Defender, so there is no rip-and-replace and no single-vendor lock-in.

HOW A THREAT BECOMES A CONTAINED CASE

01

We watch.

24x7 monitoring across your logs and endpoints.

02

Automation triages.

Enrich, correlate, and collect evidence across 750+ detection triggers before an analyst picks up.

03

A senior analyst investigates.

Banking-fluent, with context from your environment.

04

We guide or contain.

Response on the EDR you already run, scoped to high-confidence critical detections, and reversible.

05

You get the evidence.

Board- and examiner-ready, mapped to NIST CSF 2.0.

FAST RESPONSE YOU CAN STILL DEFEND

Automation runs across DefenseStorm's custom detection trigger library, speeding up investigation before an analyst picks up the case: enriching the alert, correlating activity, and collecting evidence so the investigation starts with context. A senior analyst makes the judgment call, with context from banking and your environment.

Automation handles volume and speed; the analyst handles judgment.

Where automated response is enabled, it is scoped to high-confidence critical detections, least-privilege, fully logged, and reversible. That is examiner-defensible, the opposite of AI that mitigates on its own.

Exam evidence, generated while we watch.

Governance reporting is a byproduct of monitoring: mapped to NIST CSF 2.0 and aligned to the exam procedures that apply to your program, with board-ready summaries organized so you know where the answer lives when an examiner asks.

We absorb the noise, so you see only what matters.

Our custom trigger library and tuning, combined with the Collaborative SOC, take in the flood of daily events and surface only the few that genuinely need your team's attention.

KEY BENEFITS & OUTCOMES

- **Coverage without growing your team.** A senior analyst has the watch 24x7, so you get around-the-clock protection without new hires.
- **Senior expertise when it counts.** You reach a senior, banking-fluent analyst every time, not a Tier 1 queue or a bot.
- **Exam evidence as a byproduct.** Monitoring produces board- and examiner-ready evidence mapped to NIST CSF 2.0, so proof is generated while we watch.
- **Less alert fatigue.** Our trigger library and tuning surface only the few events that need a person, so your team stops drowning in alerts.
- **You keep control.** A Collaborative SOC, not a black box: you see every case and every detection, and the decisions that are yours stay yours.

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 to notify your team, under 8 minutes for critical	**98%+** of tested attacks detected (independent pen testing, trailing 365 days)	**24x7x365** US-based coverage, or After-Hours if you prefer
750+ detection triggers, fully viewable	**200+** banks and credit unions	**Built for Banking** banks and credit unions only, since day one

GIVE YOUR TEAM BACKUP TONIGHT

See what around-the-clock coverage from a banking-only SOC looks like inside your environment.

GET A DEMO | TALK TO A SPECIALIST

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