

LogicHub for Community Banks and Credit Unions

Automation-driven managed detection and response

Organizations with fewer than 1,000 employees are disproportionately damaged by data breaches. According to the 2019 Cost of a Data Breach Report from the Ponemon Institute,

an average data breach costs:

- **\$3,500 per employee** for small organization (<1000 employees)

Versus

- **\$210 per employee** for large organizations (>25,000 employees)

And average costs are **50% higher for financial institutions**. As a smaller organization, your proportional risk is substantially higher than a large bank, and you still need to deliver the same level of protection, including:

- Continuous monitoring for compliance
- 24x7 protection from advanced threats
- Documented incident response processes

But without the resources to fully staff and operate a 24x7 enterprise SOC, it's difficult for your team to build an effective security operations program and keep up with the overwhelming volume of potential threats and associate alerts on your own.

The LogicHub Solution

LogicHub partners with your team to deliver 24x7, fully managed, automation-driven detection and response. Our expert security analysts work with you to :

- Develop playbooks that *analyze event and alert data from any platform*
- Deliver detection and response *playbooks mapped to the MITRE ATT&CK framework*

We'll work directly with you to build automated threat detection and incident response processes and playbooks, dashboards and other content that maps to any other specific regulations in the way that you need, such as:

- Gramm-Leach-Bliley Act (GLBA)
- Guidelines from FFIEC and/or NCUA
- The NIST Cybersecurity Framework
- SIEM, EDR and Other Alert Triage
- MDR for cloud productivity (G-Suite, O365, etc)
- Detect and quarantine infected devices

We also ensure that your customers' data is protected. We support strong multi tenancy and we can create automated processes for obfuscating PII to ensure customer privacy and meet your regulatory requirements.

What You Need

- Cost effective, 24x7 protection from advanced threats
- Continuous monitoring of endpoint, network and user related log and event data
- Formal incident response processes that meet industry requirements

What LogicHub Delivers

- 24x7 expert detection and response services mapped to MITRE ATT&CK
- Custom playbooks and processes built to your specific requirements
- Security outcomes that eliminate alert fatigue and empower your security team

LogicHub Automation-driven Managed Detection and Response

No matter what your size or specific requirements, we'll deliver the solutions and services you need **at a fraction of the cost** it would take to do it on your own.

- **24x7**, automation-driven managed **detection and response**
- **Out-of-the-box integration** with your security stack, your processes, and your people
- **Continuous monitoring** for all of your security log and event data
- **Expert-defined content and playbooks** mapped to your specific requirements
- Dedicated team of **expert-level analysts who know your specific needs** investigating every credible threat
- Optional, **fully managed, cloud-based SIEM** for compliance
- **Complete transparency** into what we're doing when we're doing it, and how we're doing it

Choosing the right MDR partner and ensuring you have the most cost effective, proactive protection is critical to the success of your organization's security program. LogicHub's automation-driven MDR+ with 24x7 expert coverage empowers you to achieve true cyber resilience.

How it works

We integrate with your existing and preferred security tools and ingest all of your log and security event data.

We Integrate With Your Tools

We build expert detection and response playbooks that adapt to fit your people, processes and technology.

We Adapt to Your Requirements

You retain control with one-click authorization over every step in the incident response process, with the option to fully automate.

You Maintain Control at All Times

We implement a dedicated SOAR+ platform to deliver automated analysis, detection and triage for new threats.

We Analyze Everything

Our 24x7 expert security analysts investigate every credible security incident and proactively hunt for potential threats.

We Investigate and Hunt

Detailed activity reports, KPI dashboards, and expert content to keep you protected and informed at all times.

We Keep You Informed

To learn more about the LogicHub MDR+ visit: logichub.com/mdr