LogicHub

Solution Brief

LogicHub for Healthcare Organizations

Automation-driven managed detection and response

Healthcare providers, insurers and business associates are among the most targeted organizations for attempted data theft. According to industry research from Ponemon and Protenus, healthcare organizations are impacted more than other industries. Key statistics include***:***

- **$7.13 million** average cost of a breach vs $3.86 million overall
- **$429 per healthcare record** vs $146 across all industries
- **187 days** to discover a breach at a healthcare organization

And yet despite the need for a strong cybersecurity program, healthcare organizations typically have lower budgets and struggle to retain skilled resources. But you're still expected to deliver the same or better level of security, including:

- Continuous monitoring for compliance and security
- 24x7 protection from advanced threats like ransomware
- Strict adherence to data protection and breach reporting

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 associated alerts on your own.

What You Need

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

What LogicHub Delivers

- 24x7 expert detection and response services mapped to MITRE ATT&CK
- Custom playbooks and processes built to meet your individual operating requirements and protect ePHI
- Automation-driven detection & response that eliminates alert fatigue and optimizes your security team's efficiency

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 to protect ePHI and other critical assets
- Deliver detection and response playbooks mapped to the MITRE ATT&CK framework

We'll adapt to you, using your preferred security stack to build automated threat detection and incident response processes and playbooks, dashboards and other content that maps to your requirements, such as:

- Support for HIPAA, HITECH and other regulations
- 24x7 logging and monitoring of access data for EHR/EMR
- Advanced threat detection and response
- Alert triage for SIEM, EDR and other security platforms
- Monitoring of cloud assets (IaaS and SaaS)
- Automated and one-click rapid response

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

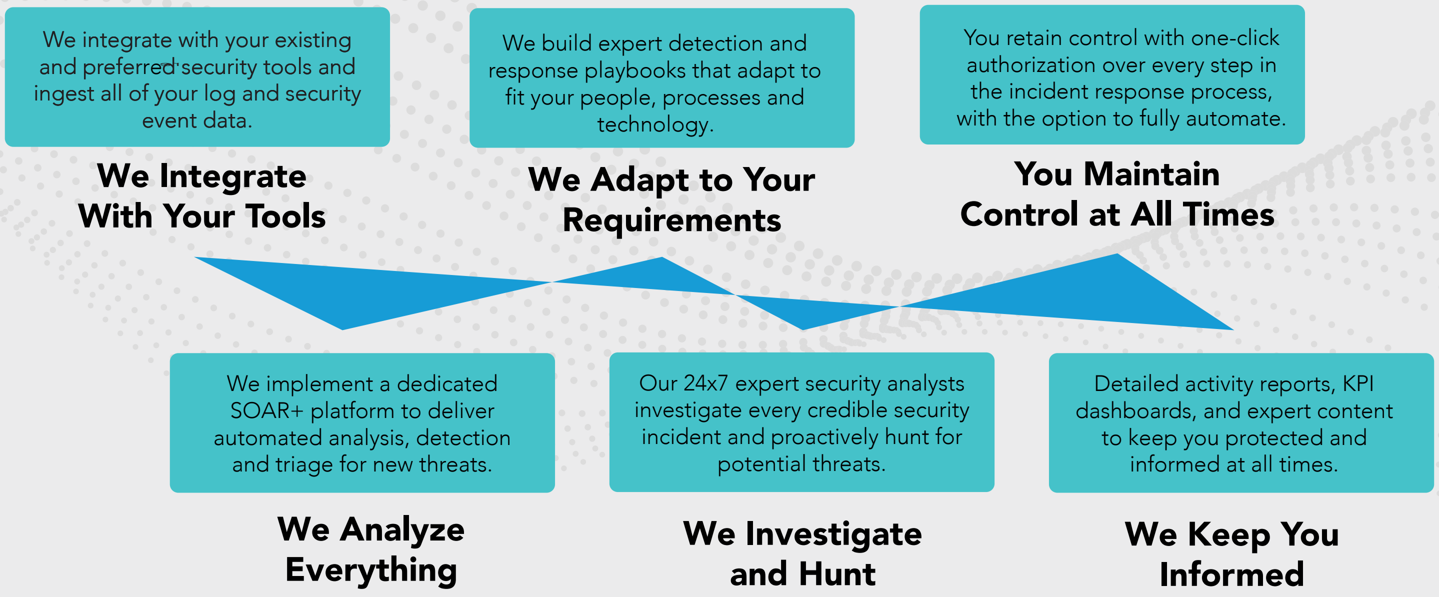
LogicHub Automation-driven Managed Detection and Response

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

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

We Analyze Everything

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

We Adapt to Your Requirements

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

We Investigate and Hunt

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

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

LogicHub
301 N Whisman Rd Mountain View, CA 94043
info@logichub.com • tel 650- 262-3756
logichub.com