LogicHub

Solution Brief

LogicHub for Small and Medium Enterprises

Automation-driven managed detection and response

Small and medium enterprises 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)

As a smaller organization, your proportional risk is substantially higher than larger, better funded organizations, and you're still expected to deliver the same level of protection, including:

- 24x7 comprehenisve detection and response for user, network and endpoint-related threats
- Protection from a broad range of advanced attacks like ransomware, phishing, and stolen credentials
- Rapid incident response processes for any critical threat

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.

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
- Around-the-clock access to skilled security analysts and expert recommendations

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

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 incident response processes, dashboards and other content that executes on a broad range of critical use cases. A few examples include:

- Phishing detection and triage
- Insider threat detection
- Detect and disable compromised credentials
- SIEM, EDR and Other Alert Triage
- MDR for cloud productivity (G-Suite, O365, etc)
- Detect and quarantine infected devices

We also ensure that your data is protected. We support strong multi tenancy and we can create automated processes for obfuscating PII or other confidential data to ensure privacy requirements are met.

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

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