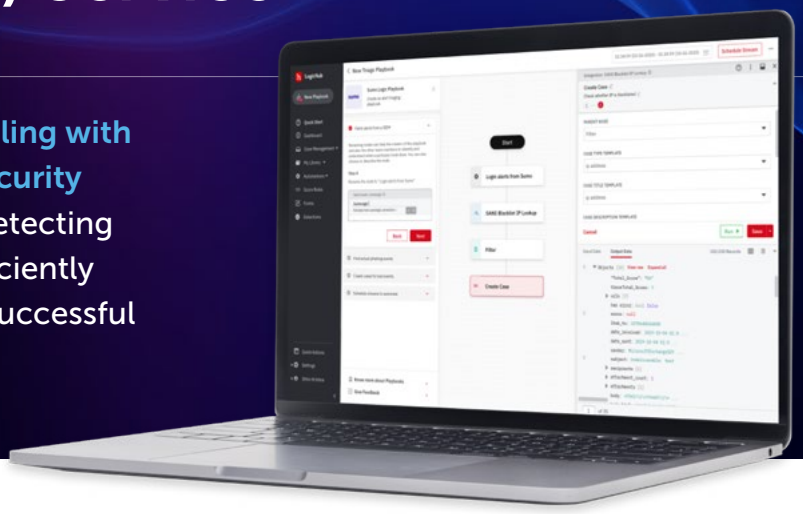
LogicHub

Solution Brief

LogicHub Managed Detection and Response (MDR) Service



Today's cyberthreat landscape requires dealing with massive amounts of data inundating our security systems. Managing alerts is one thing but detecting and responding quickly, accurately, and efficiently with actionable intelligence is the key to a successful security operation.

AI and Automation Driven Detection and Response

LogicHub is an industry leader in threat detection and intelligent response. We based our platform on expertise automation and a blend of expert systems with deep neural net architecture, designed to work with a reduced amount of data.

LogicHub advanced artificial intelligence (AI) and automation mirrors and enhances the cognitive and intuitive approach of expert security analysts – but at machine speeds and machine scale.

Because humans alone are not good at analyzing thousands of security alerts or picking out a threat from millions of data points. By combining advanced AI/ML technology with our highly experienced 24/7 service experts, we eliminate the noise, escalate only what's important, and allow you to focus on critical events and running your business.

LogicHub's unique and award-winning MDR service is powered by a highly advanced AI and automation-driven platform.

LogicHub technology is built on a progressive machine learning model that is encoded with the techniques and expertise from the best security minds in the industry and incorporates ongoing feedback from data and analysts.

LogicHub automates security operations by having machines take on the massive amounts of data generated by security tools. They quickly analyze, contextualize, and respond – at machine speeds and machine scale – 24/7/365.

The LogicHub Difference

LogicHub MDR is a true force multiplier, augmenting your team with faster analysis, detection and response, automated and threat hunting, and 24/7 expertise at a fraction of the cost.

1. Support for Your Entire Security Stack & Integrations

LogicHub is vendor and data-source agnostic. LogicHub is vendor and data-source agnostic. Our technology can connect to any tool you have in your environment via automation. Even better? We're fully agent-less, which means we won't touch your production environment. We have hundreds of integrations available out of the box, and if you have a tool that we don't support, we will provide you that new integration in less than (3) weeks at no additional cost.

2. Deep Threat Detections

LogicHub has more than 600 prebuilt detections using the MITRE ATT&CK® framework, with more added every day. We provide tailored responses on a standardized system, which contrasts with other vendors' generic, opaque content. And if you need custom detections, we'll build them at no additional cost.

3. Rich, Actionable Cases – Not Noisy Alerts

Our playbooks are designed to generate contextualized cases, not alerts. We consolidate alerts into cases and only escalate the most critical threats for customers to make decisions. Our service includes built-in case management in which we provide the case with full documentation of why we think it's a case. Then and only then do we send it over to you for review.

4. One-Click Automated Response

The LogicHub business model is built on full operational transparency for our clients, and you retain full control and visibility. We don't just monitor – we recommended actions with one-click responses delivered for your approval. Other vendors often do not provide remediation recommendations, leaving actions entirely up to customers.

5. 24/7/365 SOC Service

With LogicHub MDR, you get L1/L2 human analyst support in case your team is too busy to handle cases during off hours or weekends. Our security experts collaborate with your team, monitor your entire security stack, and build custom content to generate cases – around the clock, 24 hours/day, 7 days/ week, 365 days/year.

Intelligent Decision Automation

LogicHub AI is built on a progressive learning model, so the engine progressively learns and updates its own logic to make more accurate decisions like a human analyst. The technology reflects the experience of our skilled human threat hunters who encoded their techniques, expertise, and decision processes, and turned them into scoring and decision playbooks.

Businesses can further customize automations to augment human capabilities that can scale to meet demands.

Partnering with Our Customers

Our expert SOC team is an extension of your security team. LogicHub's outstanding team of security experts are some of the best in the business. They have decades of experience in threat hunting, detection, and response techniques, and have developed some of the most advanced playbooks in the industry.

Our clients enjoy full operational transparency and direct access to our customer success team who understand and advocate for your businesses' unique architecture and requirements. We are driven to deliver the best customer service in the industry and meeting the needs of the clients we serve.

LogicHub Helps Businesses Overcome

- Limited Threat Visibility
- Shortage of Time, Staff & Resources
- Lack of 24/7 Monitoring

About LogicHub

Founded by seasoned cybersecurity veterans from ArcSight and Sumo Logic, LogicHub is built on the principle that every process for threat detection and response can and should be codified and automated. LogicHub's managed detection and response (MDR) service is built on the LogicHub XDR/SOAR platform, which can be leveraged as a service or deployed as an independently managed platform.

LogicHub delivers intelligent automation-driven extended detection and response solutions that are flexible enough to fit any customer's requirements. LogicHub solutions adapt and grow with our customers as their needs change, delivering deeper detection, faster response, and lower dwell times.

LogicHub

Automate 99% of the threat lifecycle management process through end-to-end security orchestration, automation and response that adapts to meet the unique requirements of any organization.

LogicHub harnesses the power of AI and automation for superior detection & response at a fraction of the cost. From small teams with security challenges, to large teams automating SOCs, LogicHub makes advanced detection & response easy and effective for everyone. Learn more at LogicHub.com.

 • 800 West El Camino Real, Suite 180 • Mountain View CA, 94040 • (650) 262-7690 • info@logichub.com