LogicHub

DATASHEET

LogicHub MDR+

Automation-driven detection and response

Effective 24x7 cybersecurity is the cost of doing business and a wide range of security controls and specialized solutions exist to protect enterprises and their data. Yet security teams are being stretched thin managing these solutions, suffering from overwhelming alert fatigue while being bogged down with reactive, low-value tasks. And a combination of analyst burnout and heavy competition for scarce resources leads to high staff turnover, which creates process and skills gaps, as well as loss of tribal knowledge.

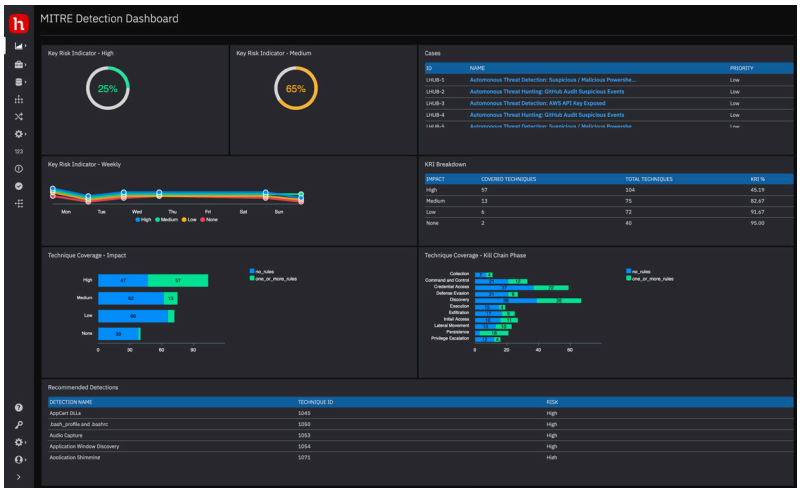
LogicHub's managed detection and response (MDR+) helps organizations like yours overcome these issues by reducing alarm fatigue, closing the resource and skills gaps, and delivering 24x7 coverage. It helps your security team extend its capabilities and gives them the time to prioritize proactive, high value activities.

LogicHub removes security barriers with adaptable and transparent MDR that is automated and always on.

LogicHub MDR+ overview

LogicHub MDR+ is a true force multiplier, augmenting your team with faster analysis, detection and response, automated threat hunting, and 24x7 expertise at a fraction of the cost it would typically take to do it on your own.

Our services are powered by the LogicHub SOAR+ platform, which delivers automated analysis, detection, and response at scale. It analyzes data from any security platform to rapidly detect and evaluate threats with greater accuracy. Automated incident response workflows use embedded machine learning to intelligently adapt to advanced threats as they occur.



With LogicHub, you gain automation-driven detection and response that provides:

- 24x7 analysis, investigation, and triage of all security event
- Faster, more accurate detection and response at machine speeds
- Access to a dedicated team of analysts around the clock
- Continuously updated, expert content

We free up your security team to spend their time applying their expertise, while keeping your network protected around the clock.

We are..

Adaptable

Your technology, your people, and your processes. No matter what you have, we adapt to fit your needs.

Transparent

We show you what's happening, when it's happening, and exactly what we're doing about it. Every step of the way.

Automated

Powered by our SOAR+ platform, we deliver fast, accurate, and consistent results, every time.

Always on

Our SOC is staffed by expert security analysts around the clock. Day or night, we've got you covered.

Managed Detection and Response Built for You

Our team of experts not only investigates threats around the clock, they continuously work with you to create and refine automated detection and response playbooks specific to your needs. These can rapidly target and defend against advanced threats, as well as perform sophisticated threat hunting. Our content delivers proactive, 24x7 advanced threat protection that is optimized to meet your needs.

What you get

Services that adapt to your existing security stack

- MDR+ and SOAR+ tailored to your preferred tools
- Custom detection and response playbooks
- Hundreds of out-of-the-box integrations
- New integrations in two weeks or less—at no charge

Dedicated client portal

- Customizable executive and KPI-based dashboards
- Easy-to-use playbook builder with built-in recommendations
- Comprehensive, interactive case management

24x7 monitoring

- Our detection playbooks analyze, investigate, and triage 24x7x365
- Our analysts perform expert investigations on every valid threat, around-the-clock
- We use your existing security stack, so you can stick with the tools you trust

Managed SOAR+

- Autonomous analysis, investigation and triage
- Fully automated or one-click incident response
- Proactive threat hunting playbooks

Scalable managed SIEM

- Optional managed SIEM with no restrictions on data
- Continuous log and security event analysis
- Compliance-driven data retention and reporting
- Ongoing expert configuration, management, and optimization

Continuously updated content

- Expert-defined and configured out-of-the-box playbooks
- Custom playbook creation and tuning
- Expert recommendations for new playbooks

Learn More

To Learn more about LogicHub MDR+, visit: www.logichub.com

The advantages of MDR+

Autonomous threat detection

SOAR+ automatically analyzes millions of events per day following the MITRE ATT&CK framework, investigating and triaging threats for faster, more accurate detection.

Our expert security analysts investigate everything relevant, reducing detection times by 90% or more.

Adaptive defense

Embedded cognitive learning allows our playbooks to intelligently and continually adapt to individual threats and unique environments. Our experts will also make customizations as needed to develop new playbooks specific to your requirements.

Cost effective 24x7x365 expert protection

Automated analysis, detection, and response ensure that our SOC is equipped to work with your team to protect your organization around the clock. Whether in-house security analysts aren't in the budget, you just can't find skilled resources, or you aren't staffed for 24x7 coverage, we've got your back with deep expertise armed with cutting-edge technology.

LogicHub

a: 301 N Whisman Rd Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756