LogicHub’s platform offers the industry’s most powerful automation platform for security operations, helping organizations dramatically accelerate every SecOps process from alert triage and incident response, to threat hunting and detection. Founded on a singular premise that every threat detection process can be automated, LogicHub empowers security analysts to be an order of magnitude more effective and productive.

**Automate Alert Triage**

*Investigate and threat rank every alert*

- Automate complex investigation playbooks quickly and easily
- Automate analysis and decision making
- Apply deep correlation and data science operators
- Reduce false positives by 95%

**Automate Incident Response**

*Contain, mitigate, and respond with confidence*

- Create automations quickly and easily
- Reduce MTTR by 10x
- Ensure consistent investigations
- Catalog evidence documentation consistently

**Automate Threat Hunting**

*Identity unknown threats in real time*

- Gain deeper proactive visibility into new threats
- Automate the expertise of the most skilled analysts to hunt unknown threats
- Prioritize top threats with the Threat Ranking Engine
- Unlike hard-coded rules, leverage the intelligence, context, and instinct of a human analyst

**Key Benefits**

- 95% reduction in false positives
- 20x faster alert investigations
- 5x better threat detection
- 3x boost in analyst productivity

**Key Features**

- Automation Engine
- Visual Playbook Editor
- Integrations Library
- Ingestion Framework
- Threat Ranking
- Advanced Correlation Engine
- Machine Learning
- Full Traceability
- Feedback Loop
- Agentless Deployment
- Smart Operators

© LogicHub 2018
LogicHub Platform

A powerful combination of automation, deep correlation, and analyst driven machine learning across all data sources.

The LogicHub Difference

The only automation platform that combines threat hunting, alert triage, and incident response.

LogicHub is the only Security Automation solution that:

- Completely automates the end-to-end SecOps processes
- Applies powerful automation flows that are more than simple “If-Then” conditions
- Features an Advanced Correlation Engine that applies deep learning across large sets of data for accurate threat ranking
- Provides a Feedback Loop for analysts to easily integrate contextual knowledge into the system
- Reduces both False Positives and False Negatives