ANOMALI®

LogicHub

MAXIMIZING YOUR SOC EFFICIENCY AND EFFECTIVENESS

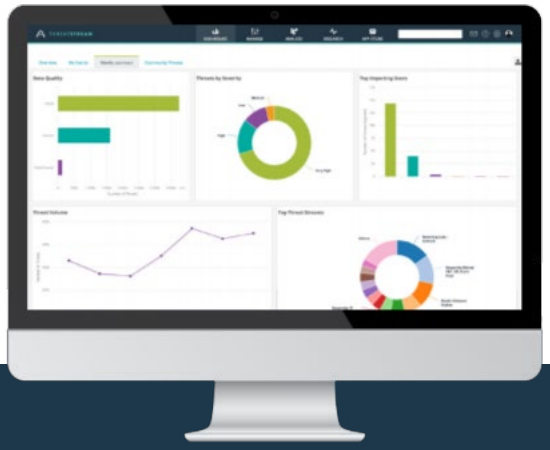
Automate Threat Detection and Incident Response with Anomali and LogicHub

ANOMALI AND LOGICHUB JOINT SOLUTION FEATURES

- **Automate Alert and Phishing Triage**
  Investigate and threat rank every alert by automating complex investigation playbooks quickly and easily as well as analysis and decision making by applying deep correlation and data science operators.
- **Automate Incident Response**
  Contain, mitigate, and respond to threats with confidence by quickly automating the process and ensuring thorough investigations.
- **Automate Threat Detection and Hunting**
  Identify unknown threats in real-time and gain deeper visibility into new threats by automating the expertise of a skilled analyst to hunt unknown threats.

IMMEDIATE TIME TO VALUE

- Reduce alerts from false positives by 95% and significantly reduce MTTR by using advanced analytics and machine learning.
- Interactive case management prioritizes the critical events.
- Integration with Anomali and other tools is seamless, rapid, and production-grade.



SECURITY AUTOMATION MEETS THE THREAT INTELLIGENCE PLATFORM

The LogicHub SOAR+ platform delivers autonomous detection and response, advanced analytics, and machine learning to automate decision making with extreme accuracy. LogicHub can automatically submit investigation artifacts, such as a URL or IP address, directly to Anomali. Anomali then returns a risk score for that artifact and LogicHub combines that score and correlates it with a range of other factors to provide a high-quality ranking of scored alerts. With LogicHub SOAR+, these threat reports can be implanted into threat detection playbooks based on Anomali threat intelligence and the MITRE ATT&CK™ framework, a globally-accessible knowledge base of adversary tactics and techniques.

CRITICAL INTELLIGENCE

Automate the process of intelligent decision making

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud

IMMEDIATE RESULTS

Focus on the truly critical incidents

THREAT DETECTION FOR WINDOWS PROCESS CREATION EVENTS

CHALLENGE:

Windows processes turn out to be a critical challenge for security analysts and Security Operations Centers (SOCs). Attackers are on the move, creating or deleting files, changing file permissions, downloading malware, creating accounts and performing other nefarious activities. Though these activities are being logged, culling through these enormous log files for indications of attacks can be time-consuming, and time is something that SOC teams never have enough of.

SOLUTION:

LogicHub Threat Detection Playbook for Windows Process Creation Events is a playbook that applies automated analysis and advanced decision-making technology analysis to identify suspicious and malicious events with the accuracy of an experienced threat hunting team. LogicHub has refined and automated hundreds of threat hunting detection patterns and techniques and mapped them to the MITRE ATT&CK™ framework and enriches these using the Anomali Threat Intelligence Platform (TIP).

CUSTOMER BENEFIT:

It typically takes months or longer and lots of work for a security team to build reliable and relevant threat detection content. The LogicHub Windows Events Creation playbook provides advanced analysis capabilities, machine-learning classification, and pattern matching built from libraries of hundreds of known attacks that can be readily deployed to your environment. This content will hone your threat detection activities while reducing the time required for triage analysis.

PHISHING ALERT TRIAGE

CHALLENGE:

When phishing attacks work, they can be devastating. Instead of proactively investigating threats, analysts spend hours per day sorting through emails forwarded to a special inbox or collected in a quarantined folder for review. Even when security analysts do an excellent job discerning phishing attacks from innocent email, there's usually no way for them to capture that expertise in a way that can be shared, automatically applied, and built on in the future.

SOLUTION:

LogicHub Phishing Triage is a security automation solution for the triage of reported phishing emails. Powered by Machine Learning (ML), LogicHub Phishing Triage rapidly and accurately analyzes emails and classifies them according to a SOC's email threat categories, such as malicious, safe, or needs further review. An intuitive interface lets security analysts quickly review results and kick-off response workflows with a click. In typical customer scenarios, LogicHub is able to achieve 97% accuracy and reduce the number of phishing alerts requiring human analysis by 75% or more.

CUSTOMER BENEFIT:

Dramatic reduction in the time required for analyzing suspicious emails which ultimately enables analysts to spend more time on proactive threat-hunting and other strategic activities. ML-powered analysis that becomes only more accurate over time, applying results from analyzing real-life phishing scenarios. Integration with other security tools for implementing automated workflows and responses. Acceleration of responses to phishing threats, reducing the risk of data breaches and other types of security attacks.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®