LogicHub

Solution Brief

LogicHub MDR and MITRE ATT&CK

Automation-driven managed detection and response

The MITRE ATT&CK framework applies years of real-world expertise of how adversary groups operate to identify common tactics and techniques to provide a holistic view of the attack lifecycle and attacker intent. Using common language, it defines a best practices approach to detecting and responding to threats, with an adaptable framework that evolves with changes in adversary behavior.

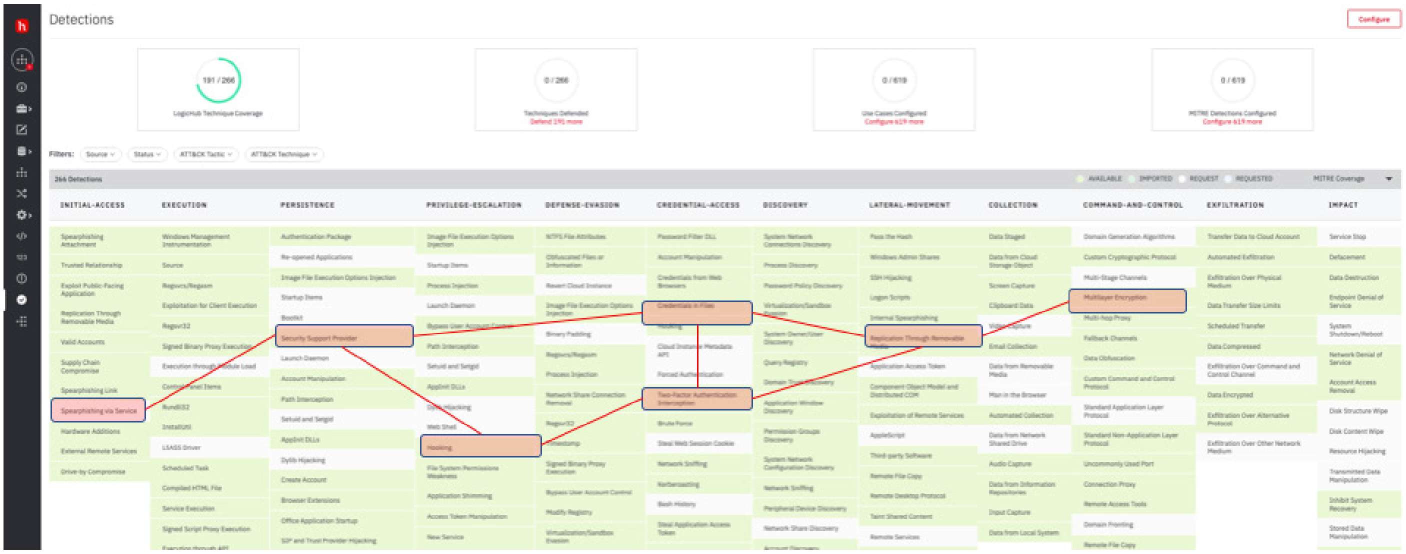
LogicHub's SOC experts are continuously developing MITRE ATT&CK-specific content, including automated playbooks that detect and respond to 100s of tactics and techniques, KPI-driven dashboards providing complete visibility into what's happening at all times, and 24x7 hands-on coverage by expert security analysts.

LogicHub's SOC is staffed around the clock by security experts and includes:

- Expert investigations of every legitimate threat, delivering **24x7 comprehensive detection and response** for cloud, user, network and endpoint-related attacks
- Incident response playbooks that suggest and/or automate **threat mitigation based on MITRE ATT&CK recommendations** and **subject matter expertise**
- **Detections for over 80% of MITRE ATT&CK techniques**

How LogicHub's Automated MITRE ATT&CK Detection & Response Works

- LogicHub ingests and analyzes all of your relevant security events and alerts
- Automated playbooks detect and record ATT&CK Tactics and Techniques in use, alerting on over 650 different vectors
- All ATT&CK-based indicators of compromise (IOCs) are retained for both immediate and historical analysis
- Playbooks automatically correlate when multiple Tactics and Techniques are used in the same attack
- Smart case creation automatically generates intelligent risk analysis based on IOCs present with complete event context
- Playbooks queue up automated or one-click incident response actions based on ATT&CK recommended mitigations
- Input from LogicHub expert security analysts, direct collaboration with customers, and embedded machine learning modules deliver a continuous feedback loop



191 / 266
LogicHub Technique Coverage

0 / 266
Techniques Defended
Defend 191 more

0 / 619
Use Cases Configured
Configure 619 more

0 / 619
MITRE Detections Configured
Configure 619 more

Filters: Source ∨ Status ∨ ATT&CK Tactic ∨ ATT&CK Technique ∨

266 Detections

● AVAILABLE ● IMPORTED ○ REQUEST ● REQUESTED MITRE Coverage ▾

INITIAL-ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE-ESCALATION	DEFENSE-EVASION	CREDENTIAL-ACCESS	DISCOVERY	LATERAL-MOVEMENT	COLLECTION	COMMAND-AND-CONTROL	EXFILTRATION	IMPACT
Spearphishing Attachment	Windows Management Instrumentation	Authentication Package	Image File Execution Options Injection	NTFS File Attributes	Password Filter DLL	System Network Connections Discovery	Pass the Hash	Data Staged	Domain Generation Algorithms	Transfer Data to Cloud Account	Service Stop
Trusted Relationship	Source	Re-opened Applications	Startup Items	Obfuscated Files or Information	Account Manipulation	Process Discovery	Windows Admin Shares	Data from Cloud Storage Object	Custom Cryptographic Protocol	Automated Exfiltration	Defacement
Exploit Public-Facing Application	Regsvcs/Regasm	Image File Execution Options Injection	Process Injection	Revert Cloud Instance	Credentials from Web Browsers	Password Policy Discovery	SSH Hijacking	Screen Capture	Multi-Stage Channels	Exfiltration Over Physical Medium	Data Destruction
Replication Through Removable Media	Exploitation for Client Execution	Startup Items	Launch Daemon	Image File Execution Options Injection	Credentials in Files	Virtualization/Sandbox Evasion	Logon Scripts	Clipboard Data	Multilayer Encryption	Data Transfer Size Limits	Endpoint Denial of Service
Valid Accounts	Regsvr32	Bootkit	Bypass User Account Control	Binary Padding	Hooking	System Owner/User Discovery	Internal Spearphishing	Video Capture	Multi-hop Proxy	Scheduled Transfer	System Shutdown/Reboot
Supply Chain Compromise	Signed Binary Proxy Execution	Security Support Provider	Path Interception	Regsvcs/Regasm	Cloud Instance Metadata API	Query Registry	Replication Through Removable Media	Email Collection	Fallback Channels	Data Compressed	Network Denial of Service
Spearphishing Link	Execution through Module Load	Launch Daemon	Setuid and Setgid	Process Injection	Forced Authentication	Domain Trust Discovery	Application Access Token	Data from Removable Media	Data Obfuscation	Exfiltration Over Command and Control Channel	Account Access Removal
Spearphishing via Service	Control Panel Items	Account Manipulation	AppInit DLLs	Network Share Connection Removal	Two-Factor Authentication Interception	Application Window Discovery	Component Object Model and Distributed COM	Man in the Browser	Custom Command and Control Protocol	Data Encrypted	Disk Structure Wipe
Hardware Additions	Rundll32	Path Interception	Dylib Hijacking	Regsvr32	Brute Force	Permission Groups Discovery	Exploitation of Remote Services	Automated Collection	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
External Remote Services	InstallUtil	Setuid and Setgid	Web Shell	Timestomp	Steal Web Session Cookie	System Network Configuration Discovery	AppleScript	Data from Network Shared Drive	Standard Non-Application Layer Protocol	Exfiltration Over Other Network Medium	Resource Hijacking
Drive-by Compromise	LSASS Driver	AppInit DLLs	Hooking	Signed Binary Proxy Execution	Network Sniffing	Network Sniffing	Third-party Software	Audio Capture	Uncommonly Used Port		Transmitted Data Manipulation
	Scheduled Task	Dylib Hijacking	File System Permissions Weakness	Bypass User Account Control	Kerberoasting	Peripheral Device Discovery	Remote File Copy	Data from Information Repositories	Connection Proxy		Inhibit System Recovery
	Compiled HTML File	Create Account	Application Shimming	Modify Registry	Bash History	Network Share Discovery	Remote Desktop Protocol	Input Capture	Remote Access Tools		Stored Data Manipulation
	Service Execution	Browser Extensions	Access Token Manipulation	Virtualization/Sandbox Evasion	Steal Application Access Token	Account Discovery	Taint Shared Content	Data from Local System	Domain Fronting		
	Signed Script Proxy Execution	Office Application Startup	New Service				Remote Services		Remote File Copy		
	Execution through API	SIP and Trust Provider Hijacking									

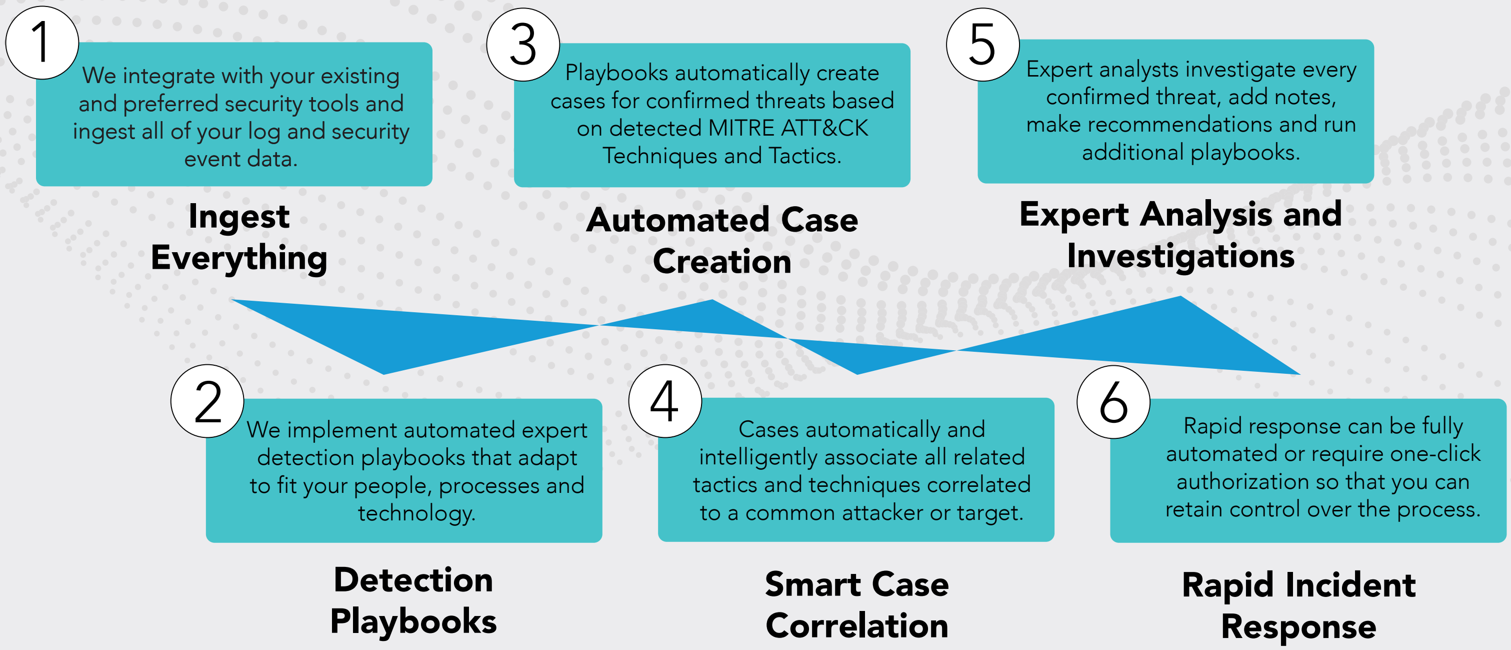
LogicHub Automation-driven Managed Detection and Response

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*** directly mapped to MITRE ATT&CK
- ***We integrate and adapt*** to your security stack, your processes, and your people to maximize ATT&CK coverage
- ***Continuous monitoring*** of all your security log and event data to ensure 24x7 threat protection
- ***Expert-configured content and playbooks*** that map to your specific operating 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, with direct visualization mapping to the MITRE ATT&CK framework

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 and direct mapping to MITRE ATT&CK delivers true cyber resilience based on industry best practices.

How it works



1 We integrate with your existing and preferred security tools and ingest all of your log and security event data.

Ingest Everything

2 We implement automated expert detection playbooks that adapt to fit your people, processes and technology.

Detection Playbooks

3 Playbooks automatically create cases for confirmed threats based on detected MITRE ATT&CK Techniques and Tactics.

Automated Case Creation

4 Cases automatically and intelligently associate all related tactics and techniques correlated to a common attacker or target.

Smart Case Correlation

5 Expert analysts investigate every confirmed threat, add notes, make recommendations and run additional playbooks.

Expert Analysis and Investigations

6 Rapid response can be fully automated or require one-click authorization so that you can retain control over the process.

Rapid Incident Response

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