SERVICE DESCRIPTION

Advanced Threat Hunting

Overview

LevelBlue's Advanced Threat Hunting (ATH) service ("**Service**") provides proactive, human-led threat hunting capabilities aimed at identifying and responding to malicious or suspicious activity within the Client's environment. LevelBlue leverages open and internal-sourced threat intelligence, behavioral indicator collection, insights derived from incident response and investigations across monitored environments, and systematic enrichment to identify both known and previously unknown threats within the Client's security solutions that are identified as in scope for the Service in the applicable SOW or Order Form ("**Client Technology**"). The following description sets out the parameters of the Service.

Core Service Features

LevelBlue Platform

LevelBlue provides a cloud-based security operations platform ("**LevelBlue Platform**") for Client to access Security Incident escalations and reporting

Onboarding

LevelBlue and Client will work together in the onboarding process and prepare for commencement of the Service.

Client Obligations

Client will:

- Procure and maintain all applicable Client Technology license(s)
- Provide LevelBlue with a list of Client's authorized user(s) for access to the LevelBlue Platform and for Service communication
- Provide LevelBlue with the necessary authorizations and permissions for LevelBlue to connect to the Client Technology; and provide LevelBlue's authorized users (as may be updated from time to time) with access to the Client Technology.
- Support connectivity and troubleshooting as requested by LevelBlue
- Work with LevelBlue to troubleshoot access to the Client Technology if necessary

LevelBlue Obligations

LevelBlue will:

- Conduct service onboarding and introduction as needed
- Enable Client's authorized user(s) access to the LevelBlue Platform
- Establish connection or access to Client Technology
- Provide guidance on communication and reporting processes

Hunt Development

LevelBlue will analyze the threat landscape across LevelBlue Advanced Threat Hunting customers and may leverage the following sources to develop a hunt package consisting of structured, intelligence-informed queries, including hypothesis-informed approaches where applicable:

- Emerging threat intelligence on active campaigns, threat actor activity, and mass exploitation
- Open-source intelligence on historical intrusion campaigns, threat actor profiles, and vulnerability exploitation
- Observed tactics, techniques, procedures (TTPs) and indicators identified through monitored and investigated client environments
- Proprietary security research and analytical, hypothesis driven analysis
- Client-requested topics where Indicators of Behavior (IoB) and Indicators of Compromise (IoC) exist and can be searched for within Client Technology, which LevelBlue may include in developing a hunt package in its sole discretion.
    - Client may request hunt topics through their LevelBlue customer-facing resource or by emailing hunt@levelblue.com with relevant information, attached documents, and links to relevant open-source intelligence

"**Business Day**" means Monday–Friday, excluding any day observed as a public holiday by any part of the LevelBlue global organization.

LevelBlue will develop at least one (1) threat hunt per Business Day.

LevelBlue may develop threat hunts on such public holidays at its discretion.

Threat Hunts

LevelBlue will leverage the developed queries to hunt within the Client Technology, and when the Service is purchased in conjunction with LevelBlue's other Managed Detection & Response services, LevelBlue may use other telemetry inside the Client's environment as LevelBlue deems appropriate.

LevelBlue will perform at least one (1) threat hunt per Business Day (as defined above) based on:

- Emerging threat activity
- Ongoing threat campaigns and vulnerabilities
- Historical findings from prior hunts and incidents
- Hypothesis based research of abuse potential

LevelBlue may perform threat hunts on such public holidays at its discretion.

Client acknowledges and agrees that hunt development and threat hunt performance are distinct activities, and the hunt performed on a given Business Day may differ from the hunt developed on that day.

At LevelBlue's discretion, select hunt queries may be re-executed on a recurring basis to identify newly observed or previously undetected activity.

Methodology

LevelBlue executes threat hunts using an intelligence-driven approach with custom and specific queries, supported by a curated and evolving query library aligned to the MITRE ATT&CK framework. LevelBlue Threat Hunters will perform deep dive analysis and research of sourced intelligence to develop queries focused on identifying Indicators of Behavior (IoB) and Indicators of Compromise (IoC), including but not limited to:

- Process execution and command-line activity
- Parent-child process relationships
- Persistence mechanisms and privilege escalation
- Defense evasion techniques
- Credential access and lateral movement behaviors
- File hashes, IP addresses, domains, file names/paths, scheduled task and services names, email addresses, mutexes, registry keys, user-agent strings, certificate names/signatures, usernames, hostnames

Queries related to the MITRE ATT&CK framework are constantly updated and refined, with coverage fitting each of the tactics categories below:

- **Reconnaissance** – Adversary is trying to gather information for future operations.
- **Resource Development** – Adversary is trying to establish resources to support operations.
- **Initial Access** – Adversary is trying to get a foothold in the environment.
- **Execution** – Adversary is trying to run malicious code.
- **Persistence** – Adversary is trying to maintain foothold.
- **Privilege Escalation** – Adversary is trying to gain higher-level permissions.
- **Defense Evasion** – Adversary is trying to avoid detection.
- **Credential Access** – Adversary is trying to steal usernames / passwords.
- **Discovery** – Adversary is trying to conduct reconnaissance internally in the environment.
- **Lateral Movement** – Adversary is moving throughout the environment.
- **Collection** – Adversary is aggregating targeted data.
- **Command and Control** – Adversary is communicating to compromised systems internally or externally.
- **Exfiltration** – Adversary is exporting stolen data.
- **Impact** – Adversary is trying to manipulate, interrupt or destroy, systems, operations and data

Triage

LevelBlue will review the data resulting from each hunt for false positives and isolate suspicious findings for deeper human-led investigation.

Hunt Analysis

Isolated suspicious findings are reviewed within the Client Technology or Client's environment, along with, but not limited to, open-source research and private sandbox executions of identified files in order to determine the severity of the associated incident. If LevelBlue discovers a significant ongoing data breach or widespread infection, LevelBlue may recommend Client escalate the incident to a digital forensics and incident response (DFIR) provider. LevelBlue will provide information and support for ongoing security events within the LevelBlue Platform and the Client Technology related to any such incident response engagement during the Term of the Service.

Advanced Analysis

In addition to threat hunting, at its sole discretion LevelBlue may perform focused, in-depth analysis in the following scenarios:

- Elevated or suspicious findings identified during hunts
- Targeted threat actor or campaign analysis
- Client-requested investigations
- Identification of potential compromise or environmental risk

Advanced analyses may include expanded correlation of activity, broader query execution, obtaining suspicious artifacts via Client Technology, and enhanced analyst review.

Security Incident Escalations

LevelBlue will create and store the output of hunt analysis where LevelBlue identifies malicious findings, vulnerabilities, and potential infrastructure deficiencies in Client's environment using security incident tickets within the LevelBlue Platform ("**Security Incident**"). LevelBlue will send Client notifications according to the Security Incident's assigned priority (see below). Security Incidents may include any of the following information:

- Summary of the incident
- Analysis
- Recommendations
- List of LevelBlue actions taken
- Request for Client to perform recommended actions

In addition, at its sole discretion, if unable to retrieve binary files and suspected malware from Client Technology, LevelBlue may request Client collect and submit those files within the Security Incident for LevelBlue's Malware teams. In such cases, LevelBlue may add any further observations, findings, or recommendations developed by this process to the applicable Security Incident.

Client Obligations

For LevelBlue to provide this feature, Client will

- retain exclusive responsibility for mitigating actual and potential threats to its environment;
- lead and execute Client processes for incident management and incident response;
- regularly update incident contacts and their respective accesses and information in the LevelBlue Platform including contact email, phone numbers, and contact order;
- utilize the LevelBlue Platform to generate secure communications, notifications, and Service feedback;

- collaborate with LevelBlue on security detection and response best practices, including Client deployed configurations, and policy definitions;
- provide initial and ongoing LevelBlue user and system remote access to the Client Technology to accommodate LevelBlue's remote analysis as defined by this service description;
- review Security Incidents, notifications, and reports as made available in LevelBlue's Platform;
- notify LevelBlue if Security Incidents, events or reports are not available in LevelBlue's Platform as reasonably expected;
- resolve each Security Incident by providing Security Incident feedback, relevant personnel, and ensuring support, and engagement of third parties, as reasonably required by LevelBlue;
- upon request, provide LevelBlue with the necessary authorizations or permissions for LevelBlue to retrieve or remove binary files and suspected malware from Client Technology for further review.
- provide LevelBlue with requested information and confirmations in a timely manner. Client acknowledges failure to do so may inhibit LevelBlue's ability to provide the Service;
- provide network documentation promptly upon request; and
- provide additional telemetry as required.

LevelBlue Obligations

For this feature, LevelBlue will

- allow authorized Client personnel (authorized by Client) access to the LevelBlue Platform to interact with LevelBlue personnel and to monitor the Service and as a repository for Client communications for Security Incidents;
- create tickets within the LevelBlue Platform to notify Client of findings and recommended actions;
- collect and process events from the Client Technology;
- analyze and raise Security Incidents, investigations, and reports identified by LevelBlue from events collected from Client's environment;
- provide recommendations aimed to improve Client's overall security posture if a hunt yields actionable findings in LevelBlue's sole discretion;
- periodically update the status of Security Incidents in the LevelBlue Platform and record communications between Client and LevelBlue pertaining to such Security Incidents;
- review Client feedback; and
- conduct further analysis on binaries that are suspicious or require reversing to validate malicious intent and gather additional indicators of compromise.

Security Incident Priority Levels

Client incident contacts defined in the LevelBlue Platform will receive communications from LevelBlue for Security Incidents via the LevelBlue Platform, email, or phone. Clients should continuously update contact information in the LevelBlue Platform.

LevelBlue assigns priority levels to Security Incidents based on factors from LevelBlue's investigation, including attack classification, SpiderLabs Threat intelligence, security outcome, derived risk, impact, and properties of the events related to the Security Incident. LevelBlue will send Client notifications according to the Security Incident's assigned priority and using LevelBlue's integrated phone and email systems (see table below). Client will document all communications, questions, clarifications, and feedback for the Security Incident in the LevelBlue Platform.

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone, Email	Security Incidents at this level potentially pose an immediate and high security risk to Client's environment, and signal an active compromise, extensive damage, or total disruption of operations to high value assets in Client's environment. Investigations that result in this priority require the Client to take immediate containment, response, or recovery actions to contain the Security Incident.
High (P2)	Phone, Email	Security Incidents at this level potentially pose a high security risk to Client's environment, and signal a potential compromise, severe damage, or disruption of operations to high value assets in Client's environment. Investigations that result in this priority require Client to take nearly immediate defensive actions to contain the Security Incident.
Medium (P3)	Email	Security Incidents at this level potentially pose medium-level security risk and signal the potential for limited damage or disruption to standard assets in Client's environment. Investigations that result in this priority require Client to take timely, but not necessarily immediate, action to contain the Incident.
Low (P4)	Email	Security Incidents at this level are not immediately actionable and may require further investigation by Client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practices.

Reporting

LevelBlue will provide Client with a consolidated report via email or the LevelBlue Platform designed to deliver visibility and clarity into all proactive threat hunt activity performed. Reports will capture data in a monthly snapshot from the first day of the month to the last day of the month, outlining the following:

- All hunts executed for the Client, with information pertaining to the hunt's title, description, source, and date of execution
- A summary and status of any Security Incidents escalated as a result of performed hunts

Problem Management

A problem is a cause or potential cause of one or more incidents impacting the health of the Service. Client agrees to report problems through the LevelBlue Platform. Client and LevelBlue agree to collaborate on problem resolution subject to LevelBlue policy.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in LevelBlue's Master Services available at https://www.levelblue.com/legal or in the applicable Statement of Work or Order Form between LevelBlue and Client.

For Trustwave Client's only:

A reference to "**LevelBlue**" in this document means "**Trustwave**".

All other capitalized terms defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.levelblue.com/legal/trustwave-contract-documents or in the applicable Statement of Work or Order Form between Trustwave and Client.