SERVICE DESCRIPTION
Priority Intelligence Service

Overview

LevelBlue's Priority Intelligence Service ("**Service**") provides analyst-led cyber threat intelligence tailored to Client's business priorities, threat landscape, and security objectives delivered via expert Q&A and reports or directly to Client's SEIM or EDR platform. The Service combines intelligence requirements development, intelligence analysis, indicator management, and operational intelligence support to help clients better understand relevant threats, prioritize defensive activities, and improve organizational intelligence maturity.

LevelBlue utilizes proprietary intelligence sources, commercial datasets, open-source intelligence, internal research, and analyst expertise to produce actionable intelligence aligned to Client's defined priority intelligence requirements (PIRs). The Service is designed to transform threat intelligence into operational outcomes through intelligence reporting, indicator dissemination, detection enhancement, and threat hunting refinement and scoping when paired with the Advanced Continuous Threat Hunting service. The following description sets out the parameters of the Service.

Core Service Features

The Service includes the following core features:

Intelligence Requirements Workshop

As a part of the Service, LevelBlue will conduct a one-time Intelligence Requirements Workshop (IRW) with Client stakeholders to establish the foundation for intelligence delivery.

LevelBlue and Client will work together to define the scope of the IRW. In general, the IRW may include:

- Identification and documentation of PIRs.
- Mapping critical assets and business priorities.
- Documenting critical applications, technologies, and appliances that could be exploited or attacked by threat actors.
- Identification of relevant threat actors, campaigns, technologies, and attack trends.
- Discussion of how to align intelligence activities with detection engineering, threat hunting, and security operations objectives.

Intelligence Collection and Dissemination

For the duration of the Service, LevelBlue collects, receives, validates, enriches, and analyzes cyber threat intelligence aligned to Client's PIRs identified in the workshop and to the applicable industry, technologies, and threat landscape.

Intelligence sources may include commercial intelligence feeds, open-source intelligence, proprietary research, observed threat activity, incident response findings, threat hunting observations, and intelligence obtained through LevelBlue's global security operations.

LevelBlue analysts evaluate collected intelligence to identify relevant indicators of compromise (IOCs), indicators of behavior (IOBs), adversary tactics, techniques, and procedures (TTPs), emerging threats, and threat actor activity applicable to Client environment.

Validated intelligence is operationalized across LevelBlue security services and may include:

- Curated and enriched IOC dissemination to Client security solutions.
- Detection content recommendations and enhancements based on identified threat activity for relevant Client or applicable LevelBlue teams to develop said recommendations to review and action.
- Providing Client or applicable LevelBlue teams with intelligence-driven threat hunt topics, including but not limited to threat actors, malware campaigns, and TTPs, hypotheses, and supporting indicators to review and action.
- Recommendations intended to improve visibility, detection coverage, and defensive posture for Client or applicable LevelBlue teams to review and action.

Intelligence Advisory Support

LevelBlue will provide Client with access to cyber threat intelligence analysts of whom Client may request guidance on cyber threats relevant to the Client's environment, industry, technologies, and security priorities.

Authorized Client contacts may submit ad hoc intelligence questions through an email to cti@levelblue.com or other approved communication channels. LevelBlue will perform limited research and analysis and provide concise responses, recommendations, context, or directional guidance designed to support operational and strategic decision-making. LevelBlue has sole discretion over which questions and how many are answered.

The Intelligence Advisory Support feature of the Service is intended for questions that can be reasonably addressed through analyst expertise and limited investigation and responded to in an email format rather than a formal intelligence report.

Examples may include:

- Is a newly disclosed vulnerability being actively exploited?
- What threat actors are currently targeting our industry?
- Is a specific IOC associated with a known threat actor or campaign?
- Has LevelBlue observed activity related to this threat?
- What defensive actions should we consider for a newly emerging threat?
- What is the significance of a recently published threat intelligence report?

Request for Information (RFI)

For the Request for Information ("**RFI**") feature, LevelBlue will provide structured intelligence research, analysis, and reporting on topics relevant to the Client's security priorities and PIRs.

RFIs may consist of either:

- Custom reports responsive to intelligence requests submitted by authorized Client personnel to cti@levelblue.com; or
- Recurring intelligence reports and assessments agreed upon during the IRW and aligned to the Client's PIRs.

LevelBlue analysts will conduct intelligence collection, research, correlation, and analysis, followed by peer review as appropriate, to produce a formal intelligence report containing findings, context, analysis, and actionable recommendations.

Monthly RFI reports are determined by the Client's purchased service tier and may be consumed through any combination of Client-requested RFIs and recurring intelligence reports.

Example RFI topics may include:

- Threat actor analysis
- Threat campaign analysis
- Industry threat landscape reporting
- Malware intelligence assessments
- Vulnerability impact and exploitation analysis
- Credential exposure assessments
- Dark web intelligence reporting

- Geopolitical threat assessments
- Technology-specific threat reporting
- Emerging threat and risk assessments

Service Tiers

The Service is available in three tiers. The applicable service tier will be indicated in Client's SOW or Order Form.

Tier 1 – Starter

- LevelBlue will provide two RFI reports per month

Tier 2 – Standard

- LevelBlue will provide four RFI reports per month

Tier 3 – Growth

- LevelBlue will provide six RFI reports per month

Service Levels

Intake Acknowledgement

- LevelBlue will acknowledge the submitted RFI requests within one business day.

Standard Delivery

- LevelBlue will provide completed intelligence deliverables within five business days following validation of the request.

Expedited Requests

- LevelBlue may, at its sole discretion, provide expediated delivery within three business days for urgent requests involving:
  - Active exploitation
  - Incident response support
  - Digital forensic investigations
  - Critical emerging threats

Client Obligations

For all the Service features, Client will:

- Participate actively in the IRW.

- Designate authorized contacts for intelligence communications.
- Provide relevant business context when submitting RFI requests.
- Provide information concerning critical assets, technologies, and priorities when reasonably requested.
- Review intelligence deliverables and provide feedback when appropriate.
- Retain responsibility for implementing any recommendations resulting from intelligence reporting.

LevelBlue Obligations

LevelBlue will:

- Conduct intelligence requirements onboarding.
- Maintain the intelligence intake and delivery process.
- Perform intelligence collection, research, analysis, and peer review.
- Produce intelligence deliverables aimed at aligning to Client priorities.
- Provide ongoing analyst engagement regarding delivered intelligence products.

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.