LevelBlue

Threat Intelligence as a Service

Tailored and curated threat intelligence for your organization.

As threat actors evolve their TTPs, generic or single-source threat intelligence limits visibility and guidance. Actionable insights and the right intelligence partner better inform decision-making.

LevelBlue Threat Intelligence as a Service (LBaaS) provides you with timely, contextualized, and prioritized threat intelligence based on factors relevant to your operations, enabling you to make risk-based and threat-informed decisions which benefit your organization. LevelBlue LBaaS is delivered using LevelBlue's SpiderLabs Intelligence Led Knowledgebase (SILK) Methodology, a human-led approach that combines expert analysis with advanced threat intelligence tooling to produce validated, high-value intelligence.

Meeting the needs of the enterprise

LevelBlue LBaaS is delivered by a pool of experienced analysts, researchers, and advisors to ensure you are supported every step of the way. LevelBlue LBaaS is a 12-month engagement that includes:

- **Initial Threat Assessment Workshop:** A collaborative workshop to identify your concerns, posture, context, technologies, and services you are dependent on.
- **Attack Surface Analysis:** Analysis of your attack surface, including domains, subdomains, and external-facing assets, seeking to identify insecure services and detect data exposure via, for example, cloud services or code repositories.
- **Intelligence Analysis:** Continuous gathering and analysis of information and insights on your organization, enabling threat intelligence to be contextualized and specific to your operations. This includes analysis of global incidents, vulnerabilities, and advisories, creating an early warning system of actionable risk-based intelligence, alongside base recommendations.
- **Dark Web and Public Internet Monitoring:** Dark web and public internet monitoring for evidence of data or credential breaches, and to identify evidence indicative of an increased threat likelihood, or information likely to impact brand or reputation.
- **Threat Knowledgebase:** Maintenance of a knowledgebase of relevant threat groups and actors, attack methods, trends, target industries, TTPs, Indicators of Compromise (IOCs), and advice on remedial activities and security controls.
- **Tabletop Exercise:** An incident response tabletop exercise to test and enhance the efficacy of your incident response processes.
- **Threat Intelligence Reporting:** Strategic, tactical, and ad hoc threat intelligence reporting, including details on threats and trends based on your industry, geography, technology, and operating environment.

Benefits

- Led by a team of LevelBlue consultants with deep subject matter expertise in threat research and analysis, providing human-led, contextualized intelligence.
- Enables risk-based and threat-informed decisions based on tailored and contextualized threat intelligence.
- Identification of insecure services, assets, and systems through attack surface monitoring and analysis.
- Analysis of dark web forums and marketplaces, and clear web activity, to identify evidence of data, credential, or systems breaches, or specific risks to your organization.
- Additional confidence through the use of multiple intelligence sources for verification and reduction of false positives.
- Fast escalation of critical information with focused, contextualized alerts delivered directly to the right contact within your organization.
- Curated analysis on current cybersecurity threats, trends, and threat actor profiles, with up-to-date regular reporting.

Threat intelligence reporting

LevelBlue LBaaS provides you with three main types of threat intelligence reporting:

Strategic Reporting: Underpins your security program to help define your security maturity and focus (e.g., industry research, observations, threat actor/group TTPs, contextual trends). This is provided on a quarterly basis.

Tactical Reporting: Informs the short- to mid-term direction of your security initiatives (e.g., identified breaches of data/credentials, exposed assets or services, vulnerabilities in your technologies). This is provided on a monthly basis.

'Imminent Threat' Alerting: Intended for immediate attention. It is based on findings assessed as presenting an elevated risk to your organization, and which may require actioning to mitigate an immediate risk. This is provided on an as needed basis.

Additional to LevelBlue LBaaS and as part of LevelBlue's Co-Managed SOC service, LevelBlue can deliver operational threat intelligence.

This separate reporting answers the question: what do we need to do now? Operational threat intelligence needs to be 'real time' and consumable to deliver immediate changes and deployment of effective controls, and typically includes observables such as IP addresses, URLs, and hashes which feed into a SIEM/SOC solution.

Analysis and research

LevelBlue will leverage a wide range of threat intelligence sources to provide you with contextualized threat intelligence. Continuous insights and data from our SpiderLabs threat intelligence and research teams are combined with OSINT, threat analysis, and intelligence leveraged from our global pool of detection, response, testing, and advisory professionals.

Consultant-led analysis

LevelBlue consultants and analysts will provide analysis, validation, and assessment of potential risks to your organization based on the available threat intelligence. This includes detailed analysis and validation of threat risks, prioritized based on their likely impact to the specific nature of your operations, as well as recommended remediation actions, updates to security controls, or suggested programs to bolster your cyber resilience (e.g., incident response training and preparedness, crisis simulations).

LevelBlue will also provide you with a threat intelligence point of contact throughout the engagement. This allows LevelBlue to build up knowledge and expertise about your organization, refining and tailoring the threat intelligence to your needs.

LevelBlue accreditations

SpiderLabs is a CREST-registered advanced security team within LevelBlue focused on application security, incident response, penetration testing, physical security, and security research. The team has performed thousands of incident investigations and penetration and application security tests globally. In addition, the SpiderLabs team provides intelligence through bleeding-edge research and proof of concept tool development to enhance LevelBlue's products and services:

- More than 25 years of industry leadership in vulnerability research and findings.
- Certified and accredited by CREST, an international accreditation and certification body that represents and supports the technical information security market.
- The first global CREST-certified member organization to identify more than 120 Common Vulnerabilities and Exposures (CVEs) and TTPs.
- 200,000+ hours of pen tests delivered globally per year and 30,000+ vulnerabilities discovered per year, including 9,000 high/critical severity infrastructure and web application sources.
- Recognized by leading industry analysts.