LevelBlue

LevelBlue Threat Hunting Program

A Proactive Approach to Countering Cybersecurity Attacks

A New Approach to Cybersecurity

Unlike most cybersecurity countermeasures, the LevelBlue Threat Hunting Program goes on the offensive to track down infiltrations. By evaluating existing security vulnerabilities, the LevelBlue Consulting Team adopts a hypothesis–based approach to testing weaknesses and eliminating threats.

The cybersecurity threat landscape presents businesses with evolving challenges. Ransomware attacks are on the rise and destructive malware continues to disrupt business operations. Better tools are required to minimize damage caused by increasingly sophisticated techniques.

LevelBlue Threat Hunting Program is a combination of strategies and proactive countermeasures that help businesses identify security weaknesses and reduce the time unauthorized users go undetected. The key lies in its unique strategic approach to anticipating and identifying vulnerabilities and verifying infiltrations. Threat hunting is the proactive analysis of network and system artifacts to identify suspicious, malicious, and unusual activity that is otherwise ignored by detection technologies. It's not a technology or a tool, but a set of protocols and methodical approaches that helps businesses lessen the impact of unauthorized access to critical systems and data.

Benefits

The LevelBlue Threat Hunting Program is designed to help your business:

- Establish a threat hunting process and lifecycle
- Create a hunting schedule
- Scope the hunt: identify objectives, outcomes, and data sources
- Encourage junior staff to participate
- Establish metrics and success criteria
- Document the hunts and the lessons learned
- Identify and address visibility and capability gaps

By evaluating a business' network and cloud resources, the LevelBlue Threat Hunting Program formulates hypotheses about which resources are most at risk, then examines those assets to determine whether unauthorized users have indeed penetrated security measures. These insights are then collected and used to refine future hypotheses and improve the prediction process. The goal is to intercept unauthorized access and limit the time users spend undetected, a factor known as dwell time.

A Goal–Based Method for Minimizing Dwell Time

The Threat Hunting Program team begins each project by examining the existing environment, including people, processes, and capabilities. These efforts start with interviews with stakeholders and include collecting documentation concerning requirements, standards, current state, and future state goals for the LevelBlue Threat Hunting Program. The team then performs an assessment of an organization to help formulate hypotheses about which assets are most vulnerable to attack.

The assessment includes:

- Threat profile and industry vertical
- Business risk identification related to cyber threats
- Threat intelligence sources and applications
- Enterprise visibility

Once the initial assessment is completed, LevelBlue begins work on developing the individual organization's Threat Hunting Program. This includes a program framework, processes, and procedures for establishing a Threat Hunting lifecycle. At the conclusion of each engagement, the team issues a report documenting the overall program, capabilities, and outputs.

These documents will help the organization perform the following security goals:

- Integrate threat hunting into their overall security program
- Establish a threat hunting cadence and reporting
- Develop dashboarding, reporting, and KPIs to measure effectiveness
- Knowledge transfer

Threat Hunting Program Lifecycle

Purpose
Why are we threat hunting?

Scope
What questions are we trying to answer?

Equipment
Data sources and tools

Plan Review
Does the plan align with the purpose?

Execute
Go hunting

Feedback
The good, the bad and the ugly

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Discover how the LevelBlue Threat Hunting Program can enhance your cybersecurity. Contact your service representative for additional information.

LevelB/ue