LevelBlue

Advanced Threat Hunting

Go beyond alerts. Be proactive. Stop hidden threats before damage is done.

Through Advanced Threat Hunting, specialized security experts proactively discover malicious activity and anomalous behavior in your network environment to mitigate risks.

LevelBlue helps you uncover previously unknown threats designed to evade detection by modern security controls, so you can neutralize active threats to your business before damage is done.

Unlike automated threat hunts for known indicators of compromise, LevelBlue threat hunters study the behavior of the most sophisticated threat actors in the world. We detect unknown threats by leveraging a human-led approach with a unique, patent-pending threat hunting methodology and platform.

Armed with the latest threat intelligence, we proactively and continuously hunt for indicators of behavior to uncover zero-days, security gaps, and hidden threats within your organization while providing actionable recommendations to mitigate potential risks to your business.

Evading modern security controls

Threat detection and prevention tools – including EDRs – based on signatures or known indicators of compromise (IoC) are not sufficient to stop sophisticated threat actors that know how to evade detection.

In 2022, "82% of breaches involved the human element, including social attacks, errors, and misuse" according to Verizon's Data Breach Investigation Report.

Attackers go to great lengths to remain undetected. Many attacks start with phishing expeditions, exploitation of unknown vulnerabilities and misconfigurations, or other social engineering schemes to steal credentials to avoid triggering alerts from existing security technologies.

After initial access, an attacker has ample time to persist and eventually move laterally within an organization's environment until the malicious task is complete and damage is done – i.e., ransomware, data-exfiltration, resource hijacking, etc.

Hunting for the unknown

Unlike threat hunting for a previously published IoC, hunting for the unknown involves looking for indicators of behavior (IoB) which lead to discovery of net-new IoCs or risks that expose you to an opportunity for compromise.

A threat hunter must diligently separate normal network activity from nefarious attacker activity. This can be a formidable task for most organizations when you're up against a sophisticated adversary that employs tactics and techniques to blend into their target environment.

Benefits

- Discover malicious activity that evades detection by modern security technology
- Neutralize covert threats to your business before damage is done
- Discover potential security gaps and mitigate your risks
- Identify insider threats and other hidden dangers
- Maximize your existing EDR investment
- Instantly benefit from findings and threat intelligence across our global client base

The task requires a human-led approach with highly specialized and tenured cybersecurity experts that must think like an attacker and have the intuition to follow the smallest detail while drowning out the noise.

An elite group of threat hunters – LevelBlue SpiderLabs®

Automation and modern security technologies alone are not a replacement for human expertise and experience. The LevelBlue SpiderLabs team of threat hunters is composed of experts with hybrid domain expertise and defensive mindsets spanning diverse security career experiences.

- Decades of career experience ranging from Corporate Information Security to Security Research to Federal and Local Law Enforcement.
- Experts in security, OS, application, endpoints, network processes and IT functions, digital forensics and incident response, malware reverse engineering, threat intelligence research, and penetration testing.
- Hands-on experience conducting thousands of threat hunts and investigations where they have encountered adversaries and honed their creative thinking skills.

Finding what others don't

Hunting for the unknown requires a threat hunter to leverage industry leading EDR technologies, customized tools, and various frameworks such as MITRE ATT&CK. The MITRE ATT&CK Framework catalogs the tactics, techniques, and procedures (TTPs) of attacker groups and can be a powerful ally when operationalized at scale.

LevelBlue's patent-pending methodology

LevelBlue SpiderLabs Threat Hunters have meticulously and continuously developed thousands of queries across multiple EDR technologies, all mapped to the MITRE ATT&CK framework.

LevelBlue's proprietary, patent-pending threat hunting framework and methodology enables our threat hunters to conduct continuous human-led threat hunts for indicators of behavior across our global client base at scale.

Threat hunting across our global client base has resulted in a 300% increase of behavior-based threat findings and allows us to detect what others don't much faster, while maximizing the value of our client's existing EDR investment. Continuous threat hunting occurs multiple times per year and each iteration becomes more laser focused on anomaly detection.

Additionally, as previously unknown threats are discovered, this information is added to LevelBlue SpiderLabs Threat Intelligence Platform to benefit LevelBlue's global client base through our products and service offerings. As new threats are discovered in one client environment, all our clients will be instantly protected.

As a byproduct of continuous threat hunting activity, threat hunters often discover misconfigurations, vulnerabilities, and other potential opportunities for exploitation. Proactively, threat hunters raise awareness to security gaps and provide recommendations to mitigate further risk to your organization.

Actionable findings and best-practice remediation recommendations

A good threat hunt is more than identifying active attackers. Advanced Threat Hunting delivers findings that can extend beyond endpoints to network traffic and security devices.

Our findings will report environmental flaws, outdated software, and network misconfigurations. When we find a threat, we work with you to take a response action. We deliver clear action items prioritized by threat level and designed to improve your overall security posture.

If active attackers are identified, you can seamlessly transition and leverage LevelBlue Digital Forensics and Incident Response (DFIR) experts to handle an emergency breach response investigation.

Get started today