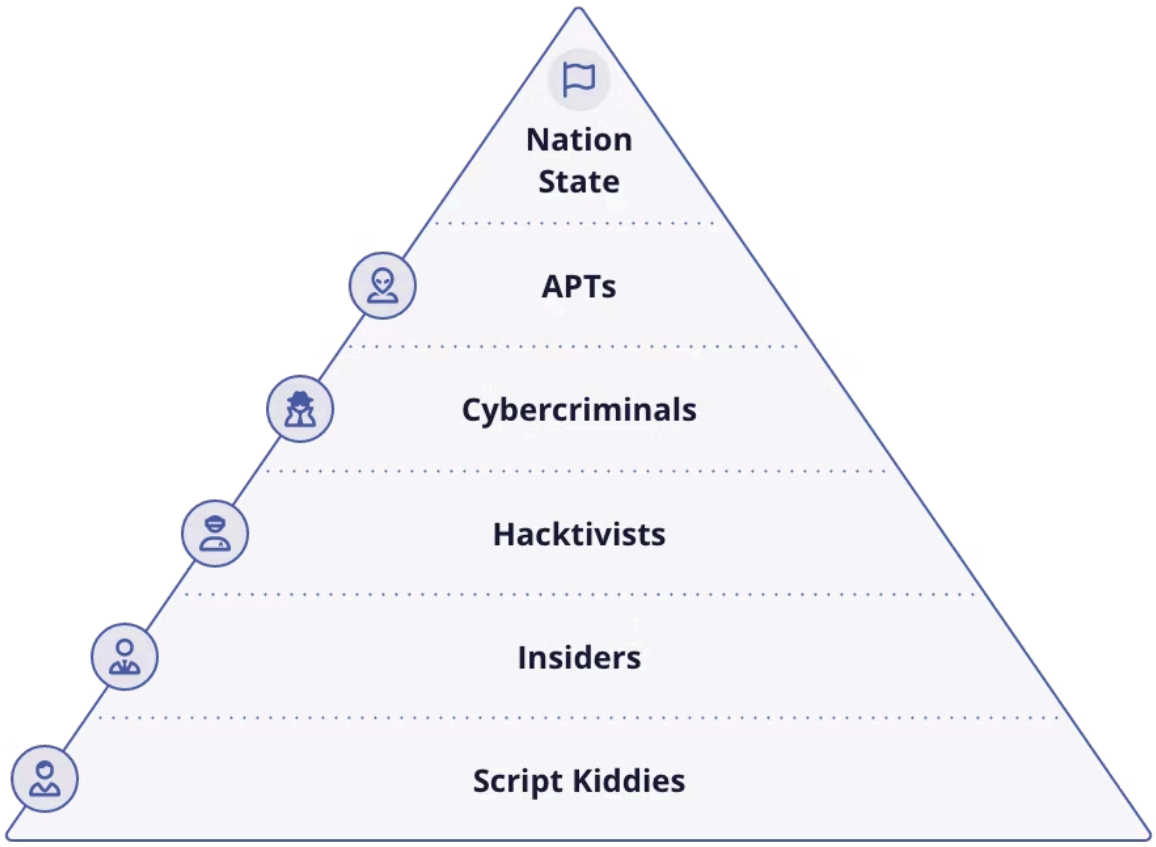
The cyber threat landscape part 5: Staying safe with multi-layered defense

BY INTIGRITI · DECEMBER 5, 2024 · LAST UPDATED ON APRIL 28, 2025

Before diving into security controls or implementing bug bounty programs, to first establish a strong foundation in risk management and define your risk acceptance criteria. Defending your assets requires identifying and mapping each asset to the specific types and levels of threats that could impact them. Security cannot be approached reactively - securing assets is a strategic effort aimed at countering well-understood threats.

The Threat Pyramid, introduced in Part 2 of this series, provides a structured way to conceptualize the hierarchy of potential attackers. At the base are low-motivation, low-capability individuals with minimal resources (often referred to as "script kiddies"). At the apex are highly skilled, highly motivated nation-state actors with significant resources and capabilities. This hierarchy underscores the need for tailored security strategies that align with the complexity and potential impact of threats faced by your organization.



We also discussed in the series how this model has evolved and how these capabilities are able to be passed down through the pyramid for financial or political gain. The ability to predict emerging threats and attribution is therefore becoming more and more difficult.

Understanding these foundational principles is critical to building robust, proactive security measures and successfully leveraging bug bounty programs.

Evolving security maturity: From basic defenses to layered controls

To truly build a robust defense strategy, organizations should first understand their risk appetite—the level of risk they're comfortable with—and evolve their security maturity accordingly. Many companies, especially in their early stages, focus on defending against lower-tier threats by relying on basic controls: firewalls, antivirus, and other endpoint protections. And while this is a reasonable start, as assets grow and attackers become more sophisticated, this level of defense simply won't cut it.

Security maturity isn't static. It's a journey, progressing from basic, easily implemented defenses to layered, more comprehensive controls that account for a variety of threat actors across the Threat Pyramid.

A mature security program doesn't stop with firewalls and antivirus software. It expands into:

1. **Basic Defenses**: Like firewalls and antivirus, which work well against low-level attackers.
2. **Advanced Controls**: Penetration testing and threat intelligence to stay ahead of skilled adversaries.
3. **Proactive Measures**: Incorporating bug bounty programs to continuously test your systems, evolving from a reactive to a proactive defense posture.

Understanding this journey is key to navigating the modern threat landscape—where your adversaries range from well-funded, highly motivated groups with specific goals to hackers in a basement who have access to tools that support sophisticated attacks.

The limitations of only applying traditional testing and scanning

While penetration testing and vulnerability scanning have long been cornerstones of organizational security, they are bound by certain limitations—time, budget, and scope. A pentest often follows a strict methodology, confined to a specific timeframe and a predefined set of assets. The goal for pentesters? Ensure that they meet coverage requirements and produce measurable results, but within the confines of those limitations.

The problem with this approach? It doesn't always provide a full picture. Pentesters, for example, might test a shiny new customer portal but completely miss critical vulnerabilities in interconnected systems that fall outside of their designated scope. Vulnerability scanning, meanwhile, is adept at flagging known issues but falls short when it comes to identifying complex, multi-step attack chains that a persistent hacker might discover.

These limitations leave gaps in your defenses. Gaps that malicious actors could exploit if left unchecked.

The unique value of bug bounty programs

This is where bug bounty programs shine. They provide an additional layer of security that traditional methods simply can't match by leveraging the power of the crowd. A global pool of ethical hackers, each with unique skills, motivations, and capabilities, tackles your systems with the same ingenuity as real-world attackers. The result? A much broader, deeper evaluation of your security posture.

Bug bounty programs stand apart in four critical ways:

1. **Unlimited Scope**: Unlike pentesting, where the scope is rigid and predefined, bug bounty programs encourage researchers to explore an organization's entire attack surface. They often discover vulnerabilities in areas that internal teams didn't even know existed—especially valuable in an era where businesses are rapidly expanding into the cloud and deploying countless new assets.

2. **Real-World Simulations**: Bug bounty hunters act much like real-world attackers, with motivations aligned with the thrill of the challenge and the potential reward. They'll spend weeks exploiting complex chains of vulnerabilities—work that's simply unfeasible in a limited pentesting engagement. This provides a more authentic simulation of how a malicious attacker might actually behave in the wild.

3. **Diverse Capabilities**: While a single pentester might excel in a particular domain (e.g., input injection vulnerabilities), bug bounty programs offer a much broader range of expertise. With participants coming from different backgrounds, you get comprehensive coverage across a wide variety of attack vectors. It's not just about finding simple bugs—these researchers dig deeper and identify hidden flaws that could otherwise go unnoticed.

4. **Continuous Testing**: Security isn't something you can check off the list once a year. New vulnerabilities pop up regularly, and with bug bounty programs, you have continuous, real-time testing. Ethical hackers report issues as they arise, ensuring that your defenses are always up to date.

Maturity through layered defense: A holistic approach

Organizations can implement a layered defense that evolves over time. A mature, layered defense involves:

- **Predictive Controls**: Using threat intelligence to anticipate potential risks and attack vectors.
- **Preventive Measures**: Such as firewalls, pentesting, and secure coding practices to minimize the attack surface.
- **Detective Controls**: Including Endpoint Detection and Response (EDR) systems to quickly identify ongoing attacks.
- **Responsive Actions**: Detailed incident response plans to mitigate damage once an attack is detected.
- **Recovery Strategies**: Post-attack recovery plans to restore normal operations as quickly as possible.

Bug bounty programs fit into both the preventive and detective phases of this approach. They act as an ongoing, real-world test of your security, helping identify weaknesses that may not be obvious or

detectable through traditional means.

Risk appetite and security maturity

When considering the adoption of a bug bounty program, it's crucial to align it with your risk appetite. Some organizations may feel apprehensive about letting "unknown hackers" explore their systems. But the reality is, malicious actors are already out there doing this—without your permission. By engaging ethical hackers through a bug bounty program, you gain control over this process. You can detect and fix vulnerabilities before they're exploited by bad actors.

Conclusion: bug bounty as the pinnacle of security maturity

Achieving true security maturity requires more than just reliance on traditional methods like vulnerability scans and pentests. The landscape is ever-evolving, and your defenses need to evolve too. Bug bounty programs offer a dynamic, crowd-powered approach to security that complements and extends beyond these conventional controls.

Incorporating a bug bounty program into your security strategy isn't just a smart move—it's the next logical step toward achieving comprehensive, proactive security. By tapping into the global hacker community, you can test your defenses under real-world conditions, uncover hidden flaws, and continuously improve your security posture—keeping you one step ahead of attackers at every level of the Threat Pyramid.

Ready to learn more about bug bounty and how we've helped customers like Microsoft, Intel, Coca-Cola and others achieve new heights in security maturity? Get in touch for a non-obligatory consultation with one of our experts today.