Guide

6 Ways to Grow a High-Performing Security Team

OffSec
The Path to a Secure Future™

Building a high-performing security team is essential for protecting your organization's digital assets and ensuring trust in your technology ecosystem. This guide outlines six key strategies to enhance the effectiveness, resilience, and alignment of your security team with organizational goals. From cultivating a customer-centric mindset to leveraging secure defaults and prioritizing continuous learning, these strategies are designed to empower your security team, streamline their operations, and foster a culture of security excellence. Whether you're looking to build your team from the ground up or optimize existing operations, this guide provides actionable insights to elevate your security practices.

1 Useful Mindsets

Be a customer-centric security team. Just as your company is building a product to serve its users, the security team should be focused on the same customer-centric goals. In some organizations, that means serving internal teams quickly and supporting secure processes. In other organizations, it means working alongside teams to develop secure products. And, always acting as a partner to help the organization reach its strategic goals while maintaining a secure environment. Ask yourself, what can you do to make their lives better? What could you do to ensure the security team has a high Net Promoter Score (NPS) with the rest of the company? Ideally, we want our security team to be seen as *enabling* the business, not slowing it down.

Make the secure way the easy way. Developers are busy and need to ship new features on a tight timeline. Even if they care about security and the quality of their code, they may not have the time to go significantly out of their way to figure out how to code securely if it would cause them to miss feature deadlines. By making the "secure way" the easiest and most obvious way to do things, we can enable engineering teams to accomplish their goals and write more secure code in the process.

For additional useful mindsets and deeper discussion, you can read Clint's TechBeacon article: Scale your security with DevSecOps: 4 valuable mindsets and principles.

2 Secure Defaults

Along the above lines, one highly effective way to make the "secure way" the easy way is by embracing "secure defaults" or "secure guardrails," or what Netflix calls the "paved road" approach. The idea is to find security-related tasks that developers must perform regularly and build infrastructure, tooling, libraries, and more that handle all of the potentially complex security edge cases automatically for them. Some common areas companies invest in building secure defaults for include cryptography, authentication, authorization, and parsing XML, as just a few examples.

For a step-by-step process in identifying where you should start investing in secure defaults and how to roll them out effectively, see these LocoMocoSec 2022 slides.

3 CI/CD Code Scanning

One of the best ways to improve your company's code security at scale is by implementing code scanning in the CI/CD process. How that typically looks is when a developer pushes new code changes into your code hosting platform, like GitHub, and then creates a new pull request (PR) so that the code can be reviewed before it's merged in, right then the new code can be scanned for security vulnerabilities before it's merged in. This way, developers receive quick and relevant feedback while the context of the code is still in their heads, requiring no context switching.

Though there are nuances, depending on your company's tech stack and culture, the following is generally an effective approach for most companies:

1. First, the security team scans a representative set of repos offline, gauging the fit of the tool to the languages and frameworks the company uses, and identifying specific security checks that appear high or low signal, disabling ones that are low signal.
2. Code scanning in CI/CD can then be initially enabled on a subset of representative repos, ideally ones owned by teams that the security team has a good relationship with so that there can be a productive dialogue and iteration process during the rollout.
    a. Initially, the security team may want to enable code scanning in "monitor only" mode where the results are sent only to the security team and not shown to developers. The goal at this stage is to get a feel for the types and volume of alerts that would be seen by developers if you were surfacing results directly within the development workflow as PR comments.
    b. After the results have been monitored and tuned, the results can be shown directly to developers as PR comments in non-blocking mode.
3. Finally, the security scanning can be rolled out to more and more repos so that all of the company's important code repos are covered.
    a. If there are specific security checks that are both very high signal and identify critical security vulnerabilities, then those may optionally be turned on to "blocking mode," where they must be fixed before the developer can merge in that code. This must be done quite carefully though, because slowing down engineering velocity or blocking developers on invalid findings can quickly damage the relationship between the security team and engineering.

For more on how ~10 companies are doing code scanning and further code scanning practices, you can refer to the same LocoMocoSec 2022 slides.

4 Elevating Teams Through Cybersecurity Learning

The threat landscape is constantly changing, requiring constant vigilance and adaptability from security teams. To minimize impact, a robust cybersecurity learning and skills development program is indispensable. Such programs are the basis for team empowerment, offering ongoing education on the latest cyber threats, technological advancements, and industry best practices. Tailoring these learning opportunities to fit various skill levels and roles within the team ensures that everyone, from the more junior-level team members to the more senior-level experts, can successfully control the impact of the next attack.

Investing in comprehensive learning and skills development not only sharpens the team's technical skills but also enhances their strategic thinking capabilities. This investment pays dividends in heightened team morale and job satisfaction, which are crucial for retaining top talent in a competitive field. Furthermore, a culture that values continuous learning equips teams to tackle new threats more efficiently, significantly lowering the organization's risk exposure. Through real-world simulations and certification courses, security professionals can continuously refine their skills, ensuring the team's evolution in tandem with the cybersecurity landscape.

By fostering an environment of continuous learning and development, organizations can upskill their existing team members to facilitate internal promotions and create a more attractive workplace that draws in new talent.

5 Strategic Recruitment and Cultivating a Robust Security Culture

At the heart of a high-performing security team lies the dual strategy of strategic recruitment and the nurturing of a robust security culture.

Strategic recruitment goes beyond assessing technical capabilities; it involves identifying individuals who are not only technically adept but also possess the soft skills necessary for team cohesion and resilience. These include critical thinking, effective communication, and the ability to collaborate under pressure. By prioritizing these attributes in the hiring process, organizations can assemble teams that are well-rounded, adaptable, and prepared to face cybersecurity challenges as a unified front.

Cultivating a strong security culture is equally critical in the context of scaling a high-performing security team, as it lays the foundational attitudes and behaviors necessary for team expansion and enhanced collective performance. Positive foundational attitudes and behaviors create an environment that is welcoming and supportive for new members. This facilitates smoother onboarding and faster integration of new team members into the existing team dynamics, enabling the team to scale efficiently without compromising performance.

6 Leadership's Role

Leadership within a security team goes beyond mere oversight; it's about inspiring, guiding, and aligning the team toward common goals while addressing the nuances of human dynamics. Effective leadership is pivotal in transforming a group of skilled individuals into a cohesive, high-performing team.

Effective management

The foundation of a high-performing team is built on clear roles and responsibilities. Leaders must ensure that every team member understands their specific duties and how they contribute to the broader security objectives. This clarity eliminates confusion and overlaps, enabling more efficient and focused efforts toward securing the organization's digital assets.

Mentorship and guidance are equally crucial. Leaders should serve as mentors, offering their expertise to foster the professional growth of their team members. This relationship encourages continuous learning and skill development, ensuring the team remains adept at navigating the evolving cybersecurity landscape.

Open communication is the lifeline of effective management. Leaders must cultivate an environment where feedback flows freely in both directions. This openness helps identify and address issues early and promotes innovation by encouraging the sharing of ideas and solutions.

Aligning goals and priorities

Understanding and prioritizing the organization's security needs are critical for aligning the team's efforts with its objectives. Leaders must have a clear vision of what needs to be achieved and communicate these priorities effectively to the team. This ensures that everyone is working towards the same goals, maximizing the impact of their efforts.

Demonstrating value is about showing the tangible benefits of the security team's work. Leaders should articulate how the team's efforts contribute to the organization's objectives, such as protecting assets, ensuring compliance, and enhancing customer trust. This not only justifies the investment in security but also elevates the team's status within the organization.

Motivating and empowering team members

Leaders' focus on boosting employee morale through a positive team culture, recognition, preventing burnout, and work-life balance is essential for scaling a security team, as it attracts and retains the talent necessary for growth and enhances team engagement and productivity.

A positive team culture is the bedrock of a high-performing team. Leaders should cultivate an environment that values respect, diversity, and inclusion. Such a culture encourages collaboration and innovation, driving the team towards excellence.

Career development is a key motivator for many professionals. Leaders should provide opportunities for team members to advance their careers, whether through promotions, new projects, or learning opportunities. This not only benefits the individual but also enhances the team's capabilities, ensuring it can meet future security challenges and scale effectively.

Conclusion

The journey to scaling a high-performing security team is complex and multifaceted, requiring more than technical expertise.

By embracing these strategies, organizations can forge teams that are not only technically proficient but also adaptable, motivated, and deeply integrated into the organizational fabric. As the cyber threat landscape continues to evolve, the strength and readiness of your security team will play a pivotal role in your organization's ability to navigate these challenges successfully. This guide offers a comprehensive roadmap for organizations seeking to enhance their security teams, ensuring they are well-equipped to protect against the ever-changing threats of the digital age.