HOW TO HIRE A STRONG AND EFFECTIVE SECURITY TEAM

KOMAND

Introduction

Your organization is thinking about building a dedicated security team, but do you know the best place to start? Before looking into the security tools you'll need, it's important to first hire the right people for the job. After all, it's **people** who will understand, manage, and use the tools in the first place.

Without people at the helm, you could quite easily end up wasting money on tools that never get used (the security tool graveyard, as we like to call it). That's why the best place to start is by investing your capital in people first. They are the foundation of a powerful and successful security program.

To get started, there are many aspects of building a team you'll need to consider, including:

- What roles do I need?
- What are their responsibilities?
- How many people do I hire?
- What are the skillsets to look for?

With all these questions, where do you even start? To remove the tedious planning involved with building a security team, we've created a framework for hiring and supporting your team to help get you started.

Who Will Do the Hiring

If you're a CISO (chief information security officer) looking to build a team from the ground up, the first hire you should make is an experienced security manager. A good security manager will have either built teams in the past or previously managed a diverse subset of security roles and skills.

Then, depending on the current size of your organization, begin planning for how the security team will grow with it, and the challenges that may come as you scale. It'll be your job to ensure the security manager you hire is equipped to help grow the team as well an effective security program.

Characteristics of a strong security manager candidate include:

- Skilled people manager
- Talented technical manager
- Understands the business implications
- Deeply experienced in either security or IT operations (or both)

Ultimately, the security manager will be the foundation of the team, and will do a majority of the hiring. They will also play an important role in developing the security strategy, toolset, and processes, and it'll be their job to make the team as productive and efficient as possible.

If you're a security manager looking to build a team and don't yet have a CISO, it's in your best interest to campaign for one early on. That's because a CISO is the security advocate in the boardroom, to other departmental stakeholders, and across the entire organization. While it may be difficult for you to convince your CIO or CEO to allocate more resources to security, the CISO can be the department champion who can make the case for the business to make that investment.

While the manager focuses more on tactical team-building and planning, the CSO can help communicate the strategy so that security aligns with what the rest of the organization is trying to accomplish. In a nutshell, if you're at the point of building a full-fledged enterprise security team, it's time to hire the visionary leader.

For organizations not ready to hire a CISO yet, the manager may take on some of these tasks, or insist on reporting to someone who understands the importance of the security function and has budget allocation power. It's not uncommon to see security teams reporting to CIOs. While not ideal, the right advocate can go a long way in ensuring your security team is successful.

How to Set Security Goals

Now that you know who will be at the helm of your security team, it's time to get strategic. Start by identifying the goals you want your security program to achieve. The goals you choose will depend on factors including:

- Industry-specific threats
- Customer requirements
- Legal and compliance directives

Knowing what you need to achieve, you can begin mapping the roles and skills that can help achieve these goals.

For example, if your goal is to protect sensitive customer information, think about the specific assets you need to protect and scenarios where your systems could be breached. Threat modeling and incident detection and response are just a few capabilities you will need to meet this goal. Threat hunting skills may also come in handy.

When it comes to goal-setting, knowing your systems, vulnerabilities, and gaps in coverage will give you a good idea of what types and levels of protection you need and how to build a security program to achieve that. Once you have laid out what your organization's goals are, you can begin building your team!

Hiring for Roles and Responsibilities

An effective security team is well-balanced, with each role complementing and supporting the others. It's okay to have some overlap in skills and responsibilities, but ultimately each role should own a specific domain.

Here are a list of key roles, the skillsets they need, and their respective responsibilities:

Chief Information Security Officer (CISO)

Security Manager

Security Engineer

Security Analyst

Chief Information Security Officer (CISO)

AKA: CIO, CSO

Whether your organization has a dedicated CISO or a general CIO, this person is responsible for defining your organization's entire security posture. The CISO plans the strategy, programs, policies, and procedures to protect the organization's digital assets, from information to infrastructure and more.

A CISO is sometimes responsible for compliance, as well, which may require additional strategies on top of the security-related ones.

Reporting to the CEO or CIO, CISOs have the most contact with the C-suite. It's their job to represent the interests of the security team to the rest of the business.

Your C-level security representative should focus on clearly communicating the business case for security, and on developing a complete strategy that covers prevention, detection, and response.

A good CISO will know and understand the information and systems they're protecting. They'll know the threat landscape and be able to identify, create, and maintain policies to help mitigate risk, as well as enabling rapid response to incidents.

CISO Responsibilities:

- Oversee the entire security digital security program
- Develop the overall security strategy
- Communicate why security matters to the executive team
- Align business goals with security
- Oversee compliance requirements
- Plan for business continuity
- Develop a plan for loss prevention and fraud prevention
- Budget and forecast for security spend
- Handle privacy concerns

Security Manager

AKA: SOC Manager, Security Director, SecOps Lead

The security manager will run your SOC or security team. This role involves creating a vision for hiring, building processes, and developing the technology stack. A security manager should have significant experience with running a security team, and should be able to provide both technical guidance and managerial oversight.

Note: In the case of no CISO, the security manager is usually top dog and will own many of the responsibilities outlined above, too. If it sounds like a lot of responsibility… that's because it is. You'll want to hire accordingly.)

Security Manager Responsibilities:

- Manage all activities of the SOC (or security team)
- Provide vision and strategy for the team's people, processes, technology
- Hire security personnel and manage career development
- Develop alert handling procedures
- Develop incident response plans
- Develop vulnerability management program
- Analyze and optimize workflows, including automation and orchestration
- Communicate security needs to the rest of the organization
- Budget and forecast for security spend (especially if no CISO exists)

Security Engineer

AKA: Security Architect, SIEM Engineer, Security Device Engineer

Depending on the size, composition, and needs of your organization, you may have a variety of security engineers and/or architects on your team. While the broadest job title is "security engineer," there may also be people on the team who specialize in SIEM, endpoint security, and other specific areas of security engineering.

This role is responsible for building security architecture and engineering security systems, as well as working closely with DevOps teams to ensure continuity and speed of releases. They should also be able to document the requirements, procedures, and protocols of the architecture and systems they create.

Security Engineer Responsibilities:

- Create requirements and documentation for security systems
- Define and document security procedures and protocols
- Configure and troubleshoot security infrastructure
- Engineer, implement, and monitor security systems
- Develop technical solutions and select or build new security tools to mitigate vulnerabilities
- Develops automation and orchestration between security tools
- Communicate security incidents to the rest of the organization
- Report on assessments, outcomes, and improvement recommendations

Security Analyst

AKA: Incident Responder, Incident Handler

Security analysts are the foot soldiers of security. Their job is to detect, investigate, and respond to incidents. They may also be involved in planning and implementing security measures and in building disaster recovery plans. Depending on the nature of your security program, analysts may need to be on-call at various times to handle incidents as they arise.

Analysts may also be responsible for recommending new technologies and installing them, as well as training team members to use them. Many organizations break security analysts out by level or tiers, where the rank determines the skill level of the analyst. Higher-ranked analysts will handle escalated events or more complicated incidents and perform proactive hunting for threats that may have escaped their alerting systems.

Security Analyst Responsibilities:

- Monitor and prioritize alerts
- Investigate and respond to security incidents
- Plan and implement security measures
- Create, test and implement network disaster recovery plans
- Perform risk assessments and testing of data processing systems
- Recommend security enhancements and purchases
- Train staff on network and information security procedures

Characteristics of Effective Hires

Certain characteristics make for a good security team member. While you will see some variation from role-to-role and person-to-person, these are good baseline qualities to look for when you are making important hiring decisions.

6 Characteristics of Successful Security Hires

1. Expertise

How do you uncover a candidates level and type of expertise? When interviewing, ask questions that will help you suss out how analytical a candidate is, how experienced they are in the role, and whether they have a problem-solving nature. Some examples of good questions to ask include:

- If we had a major security breach tomorrow, what would you do?
- What's your philosophy on security?
- What are the best decisions you've made in your security career? What would you go back and do differently?
- What are the biggest challenges you've faced so far and how have you addressed them?

2. Discipline

Security requires speed and accuracy, so discipline is a key trait to look for. The more disciplined a security practitioner is, the more likely they are to approach challenges methodically and to help the organization ensure its overall security posture is strong.

3. Pride (But Not Ego)

You want to work with security folks who are proud of what they do, know the value of their work, and are motivated to succeed by not only internal drive but also external expectations. While you don't want someone who thinks they are above everyone else, pride in what they do is a great characteristic to look for.

4. Passion and Motivation

On a related note, it's important to look for security team members who are passionate about what they do, because they will be the most motivated to perform. Yes, you can incentivize someone with a fat salary; no, it won't make them work harder. When interviewing, look for people who genuinely enjoy what they do.

5. Collaboration

Security is a team sport. While a strong individual player can be a boon, if people don't collaborate well, it's unlikely that your overall security posture will be as strong as it could be. When interviewing, look for respectful, empathetic team players who understand that a team is better when everyone works together.

6. Mentoring

A way to bridge the security-talent gap is to build a team that mentors and supports its junior members, enabling them to grow into more advanced roles. Look for people who genuinely enjoy this aspect of the job, as they will help build an overall stronger team.

Scaling Your Team

Going from a small security team to a large one isn't as simple as hiring more people. Instead, you need to be able to scale particular aspects of your security organization. Here are three key areas you should focus on when it comes to scaling your team.

Talent Sourcing

Good security practitioners do not grow on trees (unfortunately). So as your team grows, you will inevitably need to look beyond the traditional hires and think creatively about who could make a good team member. As we mentioned in the Characteristics section, mentorship can help you level up your team's skills.

While it would be ideal to hire people who have degrees in security and already know what they're doing, it's not a bad idea to look outside of the traditional technical degrees. If you go after people with the right characteristics, you can often train them to be highly effective security team members.

Training

Hiring the right people is the first step, but training them in the ways of your company and your industry is almost as important. The good news is that you don't have to do this alone. There are many resources out there today that can help you take your

team's raw talent and mold it into the skills and practices that your organization needs.

SANS, for example, provides excellent courses and certifications, both online and in-person, so that's a good place to start. There are also open communities, such as PeerLyst and the Komand Komunity, dedicated to sharing knowledge and training new and existing security practitioners.

Just remember that while certifications are helpful, they are not always a key indicator of talent or ability. Much more important are personality characteristics, experience, and passion.

Retention

Burnout is a reality in pretty much any industry, but it's especially apparent in security. No one wants to stare at a dashboard full of false alarms all day, every day. To avoid alert fatigue, a strategic combination of orchestration and automation can take the human element out of the most boring and tiresome aspects of the job.

Finally, make sure that the work your employees are doing is well aligned with their career goals and that you take a genuine interest in their overall career trajectory. The reality is that people last much longer at organizations where they feel that management actually cares about their path and gives them meaningful work that is well-suited to their skills.

People › Process › Technology

At Komand, we're big believers in hiring the right people first and foremost. While it's fun to pick out new tools that will support your overall security posture, it's best to have the right people on board before you do so. People, process, and technology are tightly intertwined in security, but it's the human element that makes it all work.

By understanding the roles to hire, the characteristics to look for in new talent, and the best ways to keep them engaged and happy, you stand a strong chance of building a team that will be successful now and well into the future, no matter what threats come your way.

Komand is a security orchestration and automation platform that gives your team the power to quickly automate and optimize security operations, with no need for code. Connect your tools, build workflows, and utilize human decisions to accelerate incident response and move security forward, faster.

KOMAND