2ND EDITION

The Early Security Engineer's First 90 Days checklist

sqreen

INTRODUCTION

Damn, but security is hard.

Being the first security engineer in a startup that already operates for a few months or even years can be quite daunting. This security checklist aims to help security engineers and CISOs in early stage companies to prioritize their efforts in the first months of their new job. Have feedback? Let us know!

Sqreen's mission is to empower engineers to build secure web applications. We've put our security knowledge to work in compiling an actionable list of best practices to help you get a grip on your security priorities. It's all on the following pages.

We hope your find if useful. If you do, share it with your network. And if you don't, please take to Twitter to complain loudly—it's the best way to get our attention.

The Sqreen Team
@SqreenIO

PROCESS

✓ Ask questions and take notes during onboarding

Regardless of the maturity of the onboarding process at your company, whether formal or informal, seize the opportunity to ask questions and take extensive notes. These will be useful as you get settled into your role. Pay extra attention to anything security-related during onboarding. You can compile your observations in a discovery report for an early win.

✓ Automate security as much as possible in the CI pipeline

If your security practices impact your development velocity, they will be looked at as more of a burden than a value. The best practices today are to take lessons from DevOps and find ways to bring security closer to developers. Leverage tools that can automate security checks and monitoring. Implementing automated SAST/DAST tools, vulnerability dependency scanning, and others will help you catch the obvious flaws before they get into production. Just beware that you'll have to sift through false positives and that these tools will not be able to identify flaws in your business logic or once your tools are in production.

Read more:
- SAST vs. DAST vs. RASP
- SAST, DAST, IAST, and RASP: Pros, cons and how to choose

✓ Automation is key

With the amount of tasks required as the first security engineer, you can easily drown under less important tasks, resulting in losing track of serious unresolved vulnerabilities and substantially diminishing your incident response capabilities. Automate as much as possible in order to free up valuable time for tasks that actually require human expertise and deeper analyses. Take advantage of the multiple solutions offered in the market and of computational analytical power.

Read more:
- Sqreen
- Security automation is maturing, but many firms not ready for adoption
- Why automation is key for the future of cyber security
- 8 Ways Security Automation and Orchestration Is Transforming Security Operations

---

✓ Be the point of contact to perform security reviews of architecture

Be available to your engineering team for security reviews of the architecture and update the architecture documentation regularly. You want your engineering team to come to you and work closely with you on the entire gamut of security needs, so be as present and helpful as possible.

Read more:
- OWASP Application Security Verification Standard Project

✓ Build a process to manage third-party services

Third-party providers and agencies need to be managed from onboarding to offboarding. This entails a thorough due diligence before and during the relationship as well as frequent risk assessments to keep abreast of the level of access the provider has and the potential vulnerabilities involved. The contract termination step is often overlooked and should be well prepared for during contract drafting, notably in terms of data migration and access removal. A checklist of all the tasks to be performed during onboarding and offboarding should be set up and regularly updated.

Read more:
- Five Steps to Effectively Managing Third-Party Service Provider Risk
- 9 Best Practices to Jumpstart your Third-Party Management Program
- Vendor Security Assessment Questionnaire

✓ Create a flag for security-related tasks

If your company has an issue tracking system (such as JIRA), make sure that security-related issues can be identified easily or work with the team managing the system to create a special flag or project. Communicate this new category to your co-workers and clarify how and when to use it. You can also use a dedicated vulnerability management system such as ThreadFix which can be integrated with JIRA.

This will make addressing and prioritizing security issues much easier for you.

Read more:
- ThreadFix Vulnerability Resolution

✓ Create a security incident response plan

Define what constitutes a security incident and design the response plan outlining the necessary tasks and roles. Share the response plan widely and make sure the employees are aware of their roles through regular training and simulation exercises. You don't want to be in the position of needing to wing it during the crucial time after a breach or major incident.

Read more:
- Awesome Incident Response
- 10 steps for a successful incident response plan
- 6 Phases In The Incident Response Plan

✓ Determine who was informally in charge of security before you joined

Even though it may not have been somebody's specific role, someone was handling security aspects for the company before you started. Take the time to meet early on with the "security champion," not only to gather precious information about the current state of things, but also to agree on his/her scope onwards should the person want to stay involved in security tasks. Depending on the company, this person might be the CTO or a security-minded developer.

✓ Enforce a process for security code reviews

Work with your developers to set up a process and a checklist for security code reviews in order to empower them to run manual and automated security code reviews themselves. Be available to answer their questions and be ready to assist if needed.

Read more:
- Vulnerability Management Process
- OWASP Code Review Guide

✓ Enforce the usage of password managers with strong password policies

With a password manager, your users will only need to remember one master password. All other passwords can be complex and long; the password manager will take care of storing them and retrieving them when needed. The password manager can also generate random strong passwords to be used.

Read more:
- Password managers: A cheat sheet for professionals
- Dashlane

✓ Ensure you are looped in on the SDLC

You should add some checkpoints to the SDLC so the developer teams will think of the security team when they're creating and updating applications. Some tools or checklists allow for asking developers a small set of questions when starting a project in order to let the security team know how much attention they should pay here. For instance, "is this service gonna be exposed on the Internet", or "Is this service handling customer data" are questions that can help you quickly get a sense of how involved you need to be on any particular project.

Read more:
- GoSDL

✓ Explore and address the security backlog (if there is one)

Oftentimes, even if vulnerabilities have been reported (in JIRA for example), they have not been addressed prior to your arrival because people did not know they had to address them, did not realize that they needed to be fixed immediately, or did not have or allocate the resources to assess and fix the issues. Getting a handle on the backlog of reported security issues and prioritizing fixes is a good place to start after you understand the systems your company has in place.

Read more:
- 7 common security bug management mistakes and how to avoid them

---

✓ Fix the most urgent issues

Do not be alarmed or overwhelmed by the number of vulnerabilities uncovered during your audits. All of them do not need to be fixed right away; you can draw up a plan to fix them over time. However, do not defer fixing the most critical issues. If you identify a serious vulnerability during one of the audits and security reviews, you should pause and fix the issue immediately. If you can't fix it, mitigate it.

✓ Implement and maintain company security policies and procedures

Draft security policies and procedures for the company, and, more importantly, communicate and circulate them. Make sure they are easily accessible and make them understandable for your co-workers. Set up a process to review and update them regularly at a certain frequency or when a specific event occurs.

Read more:
- 9 policies and procedures you need to know about if you're starting a new security program
- The Key to Better Cybersecurity: Keep Employee Rules Simple
- Drafting Cyber Security Policy for your Company

✓ Include security in the onboarding/offboarding process for employees

Onboarding and offboarding are important security moments for your company. You'll want to ensure that new employees enact the security measures needed and that your company follows the appropriate steps for employees who are leaving.

Your onboarding checklist should contain a list of all the steps you and they need to follow when an employee, contractor, or intern joins your company. A similar list can also be used when someone is leaving. Ensure that you deprovision all accounts they had access to during the offboarding.

Read more:
- Awesome onboarding
- Rippling

✓ List and prioritize your security issues

Compile all the issues you uncovered during the general and specific security audits, then prioritize them by risk. Setting up a vulnerability management system will be helpful.

If no security issues are in the backlog... there is probably a cultural flag here!

Read more:
- Vulnerability vs. risk

✓ Prepare the groundwork for external security tests

Before embarking on independent security assessments and penetration tests, it is good practice to run checks and correct some commonly identified issues (such as missing patches, weak or default passwords used, unsupported operating systems or missing input/output data validation) in order to use the external auditors time and expertise on more subtle issues.

Read more:
- 10 Tips to Reduce Common Vulnerabilities Exploited by Cybercriminals
- How to Fully Leverage your Pentest
- 10 steps to managing a successful network penetration test

✓ Set up and facilitate a public bug bounty program

A bug bounty program will allow external hackers to report vulnerabilities. Most of the bug bounties programs allow you to offer rewards for bugs found. A lot of the reports won't be valuable and you need security-aware people inside your development teams to evaluate the bugs you receive. These programs are good additions to other security initiatives as it incentivizes people outside your company to share bugs you may have overlooked.

Read more:
- Launching an Efficient and Cost-Effective Bug Bounty Program
- Hackerone

✓ Structure and be the technical resource for your sales team and customers

As a security engineer, you might also be the go-to resource for sales teams that require help filling in security forms. Spend some time retrieving and structuring all the previous requests to save time for future questionnaires.

Read more:
- CSA - Cloud Security Alliance

✓ Take time to learn the specifics of your new company

Don't just take your previous experiences at past companies as the go-to model for your new company. While some things will be the same, several aspects will undoubtedly be different, and doing exactly what you've done before won't be as effective. If you're coming from a more mature company, it's easy to suffocate an agile startup with heavy security that does not scale well, for example. Security engineers operate inside a business, and understanding that business before enforcing GovAgency-like security measures is key.

✓ Understand how product development happens in your company

As part of your first week exploration, you need to gather enough information from key stakeholders in order to have a clear understanding of the product development processes (e.g. steps, key milestones, teams involved, governance structure, etc.). These might be catalogued in documentation or through detailed oral explanations that should be written down. Deeply understanding the product development processes and structure of the engineering organization in your company will serve as a basis when you start to introduce security awareness and tasks within the product development lifecycle.

Read more:
- Spotify squads
- Scaling the engineering org at PagerDuty

CULTURE

✓ Be humble and respectful - Kill the shame game!

As a general rule of thumb, adopting a humble and respectful demeanor is a factor of success for every newcomer within an organization. It's tempting to show off how much you know about security and cyber-splain to everyone how insecure their setup is, if only out of a desire to establish your authority and credentials. But this will backfire on you. Being too hasty and judgmental in pointing out the shortcomings in the company's security will not earn you the respect of your new colleagues, rather it will drive them away. Take comfort in the fact that if the company deemed there were no issues, you would not have been hired!

✓ Build relationships with key stakeholders

If it was not included in your onboarding documentation, ask for a list of the key stakeholders in your organization, be they developers, ops, execs, or managers. Your manager might see the importance of accompanying you to introduce you. Arrange together to meet with them and discuss their understanding of security, your role, and their concerns.

✓ Don't create a security awareness program (they don't work) but...

... enable and infuse a security culture

Don't make security a one-day annual training everyone has to go through and then forgets about. Permanent and contract employees need to be aware at all times of security threats, beginning with how they set and handle their passwords, use their emails, and secure their laptops and external drives.

Read more:
- The Fundamental Flaw in Security Awareness Programs
- 7 elements of a successful security awareness program

✓ Hold security trainings for engineers and non-engineers

Liaise with your people team or your CTO to set up a targeted security training for all employees, whether they're engineers or not. The training should not be just a list of instructions, but rather a clear explanation as to why certain rules have to be put in place. You can include technical details if necessary, but make them accessible for all skill levels. The training should be included in the onboarding process.

Getting buy-in on the security policies you're implementing will make them much more effective, and a good, empathetic training will help you do that.

Read more:
- Good security trainings

✓ Meet with fellow security engineers from similar companies

The security community is generally a friendly one, and you can learn a lot from other security-minded professionals. As such, if you are not already a member of a professional group in your area, look for security meetups and communities, both online and offline. You could also reach out directly to fellow security engineers, whether in the same business line as you or not, to exchange ideas about your jobs and responsibilities or to discuss how they navigated being one of the first security engineers in their organization, if they were.

Read more:
- AppSec meetups
- Information Security Community (LinkedIn group)

✓ Never stop learning!

Managing security is an ever-changing landscape, so you need to keep yourself updated on the practices, tools, zero-day vulnerabilities, patches etc. It can seem overwhelming, but there are many websites and newsletters in which you can get regular information.

Read more:
- Sqreen blog
- OWASP Top Ten Project
- AppSec USA
- Down the Security Rabbithole
- Inside security

APPLICATION SECURITY

✓ Add a security policy to the website

When security researchers discover vulnerabilities in the web services of your company, they will need a way to report them properly to you. By adding a security policy, such as security.txt, to your website, you help them easily get in touch with you about any security issues they uncover. You should mention that you support responsible disclosure, allowing you time to assess and fix the reported vulnerabilities.

Not having a clear means to communicate security vulnerabilities will either mean that they won't get reported, or that they will get lost in the shuffle of your company's generic "contact us" inbox.

Read more:
- Open Source Security Page
- https://securitytxt.org

✓ Audit your DNS settings

As more and more day-to-day business activities and revenue rely heavily on access and interactions with your website, it is important to audit your DNS as soon as possible and regularly afterward. Without proper security on your DNS, attackers could extract a list of all your assets or steal your domain names, which means they could lead efficient phishing attacks on your customers.

Read more:
- Eight reasons why you should conduct a DNS audit

✓ Audit your applications

Application security is increasingly one of the top security concerns for modern companies. On early audit you'll need to do is on your applications. You'll want to gather answers to questions like:
- Are your applications using vulnerable or outdated dependencies?
- Are they accessing the database?
- Are they handling authentication?

Do they rely on a framework (Rails, Symfony) or are they using in-house components?

Read more:
- Use Sqreen during your audit to find and remediate issues faster
- Web Application Security Testing Cheat Sheet
- OWASP Top Ten Project
- Auditing Applications, Part 1
- Auditing Applications, Part 2

✓ Enforce two-factor authentication

Everyone at your company should use 2-factor authentication. By adding 2FA, you add an extra layer of security. Should your coworker's password get stolen, the attacker would still be locked out unless they have access to the second factor (e.g. phone app or text) as well. Phones are the most commonly used device for second factors, and thus have to be secured accordingly (e.g. with codes or biometry). Another option is to use purpose-built hardware-based 2FA, like Yubikeys.

Read more:
- Duo Security
- Auth0
- What is two-factor authentication (2FA)?

✓ Ensure that your dependencies are secure

Infuse security into all steps of the product development process and not just at the testing phase. Security-minded developers should check the dependencies in your applications for known bugs and vulnerabilities before using them and keep them updated when zero-days are found or patches are available.

Read more:
- 13 tools for checking the security risk of open-source dependencies
- Security alerts on Github
- Sqreen
- Snyk

✓ Help engineering and business teams protect sensitive business logics

The attacks representing the most significant business risk for organizations are often attacks targeting sensitive business functions of applications rather than common vulnerabilities. Work with business and engineering teams to identify the biggest threats and implement monitoring and protection solutions to automatically remediate these threats.

Read more:
- Use security playbooks to protect your business logic

✓ Make sure everything is properly encrypted

When it comes to cryptography, don't roll your own. Use accepted standards instead. Encrypt everything, including computers and mobile devices handed out to employees during the onboarding process. Turn on encryption for onsite and cloud backups. Use HTTPS to protect the users of your applications.

Read more:
- Let's Encrypt
- Microsoft encryption
- MacOs encryption

✓ Protect your applications in production

Doing as much as you can to catch security vulnerabilities pre-production is helpful, but without the full context of runtime, you won't be able to catch everything. Protecting and monitoring your applications in production, in real time, can greatly improve your security posture. Tools like RASPs and ASM platforms can give you visibility into the security of your production applications and help you stay on top of what's going on.

Read more:
- Sqreen

✓ Retrieve and audit your backups or set up new backups

In today's business world, company data is the most precious asset and backups are therefore crucial. Check the integrity of previous backups and make sure the settings are correct for future backups with sufficient storage space and backup frequency. If there are no backups, set them up immediately.

✓ Secure your emails with DMARC

Emails are usually a weak spot for attacks, especially via phishing and spoofing. A single email can do serious damage if it hits the wrong person at the wrong time. You can implement DMARC (Domain-based Message Authentication, Reporting and Conformance) to help protect your users from fraudulent emails. DMARC can be the technical support element to the security training you should be holding to help your co-workers spot and avoid dangerous emails.

Read more:
- DMARC
- How to Set Up and Implement DMARC Email Security
- Build Your DMARC Record in 15 Minutes
- OnDMARC

✓ Structure secrets management

Secrets, such as private keys, are extremely sensitive data and must not be stored unprotected. They should be securely stored in a vault. Some vaults can manage certificates as well.

Secrets committed in an application's source code should also be tracked down and stored elsewhere.

Read more:
- Vault Project
- AWS CloudHSM
- OWASP key management cheat sheet
- An Introduction to Managing Secrets Safely with Version Control Systems
- TruffleHog

✓ Think about centralized authentication

The benefits of centralized authentication for users is having a single set of credentials for all their applications. From a security standpoint, it enables you to handle only one account and gets rid of the risk of forgetting to disable an account during offboarding. It also saves time during onboarding by getting rid of the need to create lots of accounts for new employees.

Read more:
- Five Lessons We Learned on Our Way to Centralized Authentication
- Centralized Linux Authentication

INFRASTRUCTURE SECURITY

✓ Protect your infrastructure from intrusions

Make sure to follow the latest security releases and update your infrastructure as soon as they become available. Having servers without public IP addresses (e.g. in a VPC) and rate limiting authentication services are some of the measures that can be implemented to protect your servers, and consequently your applications.

Read more:
- Sqreen
- ThreatStack
- 7 Security Measures to Protect Your Servers

✓ Start thinking about physical security and hardware protection

Attackers can do a lot of damage very quickly if they get physical access to your company's or employees' hardware. Assess the risks for your company's hardware and implement some best practices around physical security protection.

Read more:
- 7 physical security practices every business should implement

---

✓ Perform a security review of your architecture

Review the elements of your architecture and the interfaces between them. Using the list of assets you were given or compiled earlier, you should be able to map the elements, draw the interconnections and identify flaws in communication protocols, servers configurations, and databases choices.

If you use Sqreen, you can also leverage the security flow map to get a real-time view of your applications and their security status.

Read more:
- Application Architecture Review
- AWS security best practices

MONITORING

✓ Assess the completeness and accuracy of your company's assets list

As a first step, assess the availability and freshness of your assets information. Is there a list of the hardware? Is there a list of the applications and services used within your company? Is there an employee directory and a list of all user accounts? Is there a list of third-party providers and their contracts? When were these lists last updated?

The employee directory might be the easiest to retrieve, as your people department should be able to provide up-to-date records with the dates of everyone joining and leaving the company. As for the other lists, you will probably have to build them or update them if they already exist.

✓ Audit your SaaS providers

Know your SaaS services! Security is a major concern when it comes to SaaS. Examine the settings and SLAs of your SaaS services, whether application, platform, or infrastructure, and compare with what was agreed to in the contracts. Take note of the flaws in the contracts to renegotiate them if needed. SaaS providers might be reluctant to be audited beyond providing documentation of their policies and procedures. Prioritize the audits requests based on the service criticality or the data sensitivity. Ensure they comply with privacy related legislation such as GDPR.

Read more:
- Audit of the top 1000 SaaS providers
- Assessing SaaS security: A top down approach

✓ Build a security dashboard

Create a security dashboard to give you an overview of the security efforts, or implement a tool that will do it for you. Avoid manual reporting -- all data should be automatically provided by the solutions you use.

Read more:
- The Top 10 Tips for Building an Effective Security Dashboard
- Sqreen

✓ Evaluate your third-party providers

Now that you have a list of your third-party providers, and a process in place for evaluating them, you should conduct thorough assessments of your existing third-party providers to make sure they are secure. Renegotiate contracts to strengthen the security responsibilities of your providers and the service levels required.

Read more:
- Security of SaaS Companies

✓ Perform deeper vulnerability testing, risk analysis and security assessments

Once you have a baseline audit of your company's security across the major areas, you should schedule deeper tests and assessments in all areas (infrastructure, applications, people). These will give you a complete picture and the baseline you need to make strategic security decisions.

✓ Perform your first security audit

Design and perform your first security audit to understand the most critical security vulnerabilities within your company. This first audit should be broad in scope but not too detailed as other more thorough audits will be performed later for specific areas. Breadth over depth here will give you a high level understanding of where the burning platforms are and what areas need your attention first.

Read more:
- How to Conduct an Internal Security Audit in Five Simple, Inexpensive Steps
- Prioritizing Your Security – Where Do You Begin?

✓ Protect against Denial of Service attacks

DoS and DDoS attacks can be devastating for a business' bottom line. Depending on your business, disruption to the availability of your service could make you lose out on revenue or impact your customers. Taking actions to protect your systems and mitigate the effects of these types of attacks is key.

Read more:
- AWS Shield
- DDoS protection, mitigation and defense: 7 essential tips
- Best DDoS protection of 2019

✓ Set up a centralized logging platform

Logs are a valuable asset for getting signals from your production environment and for investigating suspicious activity or a security breach. A centralized log platform helps you to make the most out of the analytics potential held in your logs and provides a view across all themes (applications, network, users, etc.)

Read more:
- Logging Cheat Sheet
- Choosing the Best Log Management Tool for Your System
- Centralized Logging on AWS
- 30 best practices for logging at scale

✓ Update or build the list of applications

If you have been handed a list of the applications in use within your company, make sure it is up-to-date. If not, take time immediately to update the information about the major applications first, and schedule some time a bit later to update the rest of the list comprehensively as soon as possible.

If there is no application list, you should prioritize building it.

Ask which employees have (or had previously) admin rights to install software themselves on their computer and identify the shadow IT within your company.

Read more:
- Sqreen's security flow map

✓ Update or build the list of devices

If you have been handed a list of the devices, make sure it is up-to-date or take time to update the exposed machine's information first and schedule to update the list thoroughly as soon as possible.

If the company has a BYOD policy, list those devices as well with the identification of each employee. If there is no device list, you should build it.

The list should at least include information such as IP, type of device, and physical location, if appropriate.

Read more:
- Mobile Device Management Best Practices
- Securing Laptops and Mobile Devices

✓ Update or build the list of services exposed to the Internet

If you have been handed a list of the exposed services, make sure it is up-to-date or take time to update the exposed machine's information first and schedule to update the list thoroughly as soon as possible. One good way to create this list is to use cloud API (AWS to list Route 53 domain names, or EC2 instances).

Read more:
- SaaS CTO Security Checklist

✓ Update or build the list of third-party providers

You will need to know every company or individual that has direct or indirect access to the company's systems or sensitive data. List or update the list of third-party providers and the contracts data. One critical piece of information is the date of contract renewal or termination and the data they have access to. You will also need to know how the provider's teams access the systems and which rights are assigned to them.

Having a clear understanding of the ways third party providers can and do access your systems and data is central to building the appropriate security measures on this front.

---

sqreen

Trusted by security teams, loved by developers.

Monitoring and protection platform made to be incredibly powerful yet very easy to use.

Unmatched security insights: Access to more detailed security analytics than ever, including app-level incidents you can act on immediately.

Instant Protection: Out-of-the-box modules protect apps against a broad array of threats. Setup takes minutes, no config required.

Easily meet enterprise compliance needs: Get access to the best controls without hiring expensive security teams or consultants.

Start your free trial at sqreen.com

Want this handbook as a PDF?
Scan the QR-code, or go to:
https://www.sqreen.com/checklists/security-engineer-checklist