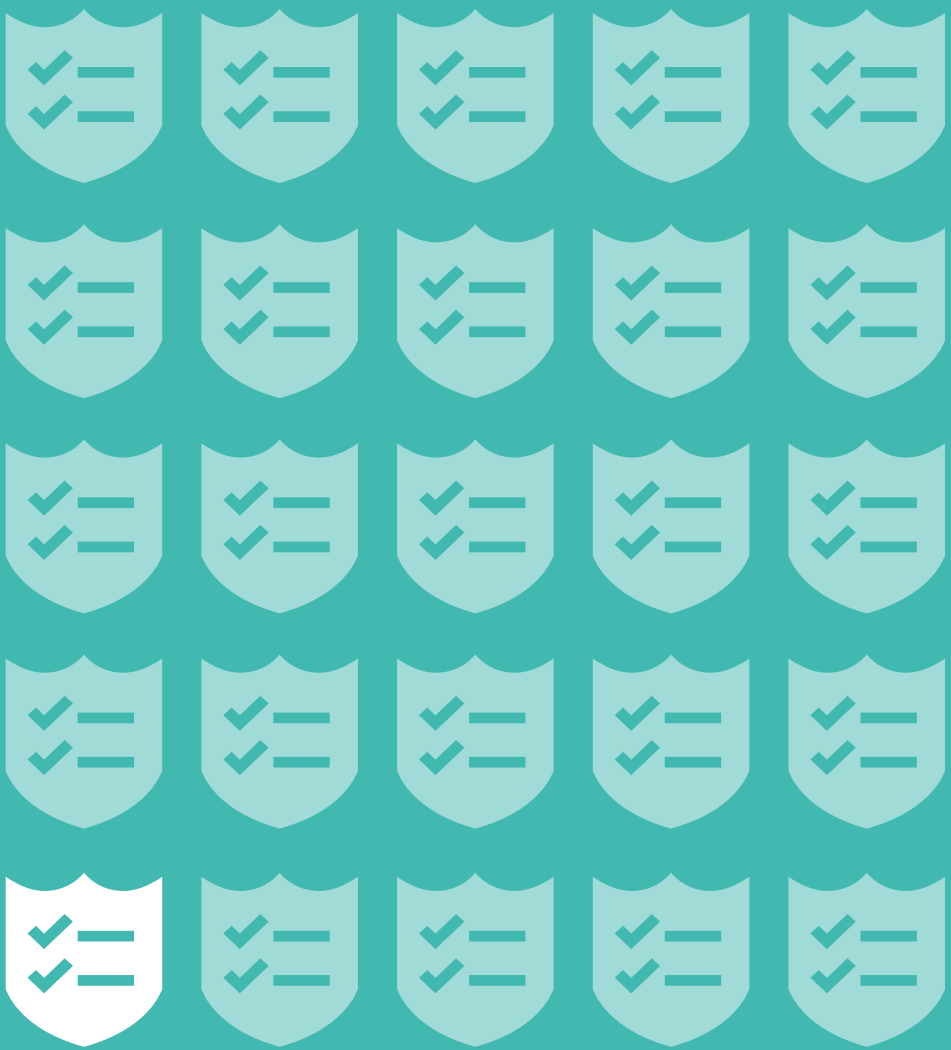

The First Security Engineer's 100-day Checklist

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 Screen Team
@SqreenIO
howdy@sqreen.io

PROCESS

✔ Automation is key

With the amount of tasks required, 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 computers analytical power.

Learn more:

- Sqreen - http://bit.ly/2MDSMTm
- Security automation is maturing, but many firms not ready for adoption - http://bit.ly/2oMthkw
- Why automation is key for the future of cyber security - http://bit.ly/2wOvVKa

✔ Build a process to manage third-party services

Third-party providers need to be managed from before 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. The contract termination is often overlooked and should be well prepared 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.

Learn more:

- Five Steps to Effectively Managing Third-Party Service Provider Risk - http://bit.ly/2NIHsuO
- 9 Best Practices to Jumpstart your Third-Party Management Program - http://bit.ly/2wSLf9q
- Vendor Security Assessment Questionnaire - http://bit.ly/2CsyaJ9

✔ Create a flag for security-related tasks

If the company has an issue tracking system (such as JIRA), make sure the security-related issues can be identified easily or work with the team managing the system to create a special flag or a project. Communicate about this new category to the employees 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.

- ThreadFix Vulnerability Resolution - http://bit.ly/2MRCqXq

✔ Create security incident response plan

Define what are security incidents and design the response plan outlining the tasks and roles. Communicate around the response plan and make sure the employees are aware of their roles through regular training and simulation exercises.

Learn more:

- Awesome Incident Response - http://bit.ly/2Q75BE9
- 10 steps for a successful incident response plan - http://bit.ly/2CDs3SH
- Security Simulations: This Is Only A Test - http://bit.ly/2Cs03RJ

✔ Determine if there are pending security tasks

Oftentimes, even if vulnerabilities have been reported (in JIRA for example), they are not addressed because people did not know they had to address them or did not realize that they needed to be fixed immediately, or did not allocate the resources to assess and fix the issue.

- 7 common security bug management mistakes and how to avoid them - http://bit.ly/2NVKovo

✔ Create a flag for security-related tasks

If the company has an issue tracking system (such as JIRA), make sure the security-related issues can be identified easily or work with the team managing the system to create a special flag or a project. Communicate about this new category to the employees 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.

- ThreadFix Vulnerability Resolution - http://bit.ly/2MRCqXq

✔ Create a flag for security-related tasks

If the company has an issue tracking system (such as JIRA), make sure the security-related issues can be identified easily or work with the team managing the system to create a special flag or a project. Communicate about this new category to the employees 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.

- ThreadFix Vulnerability Resolution - http://bit.ly/2MRCqXq

✔ Determine who was informally in charge of security

Even though it was not within an official capacity, chances are someone was handling some security aspects for the company. 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 stay involved in security tasks.

✔ Enforce a process for security code reviews

Work with the 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.

Learn more:

- Vulnerability Management Process - http://bit.ly/2NoZTij
- OWASP Code Review Guide - http://bit.ly/2NltKbo

✔ Fix the most urgent issues

Do not be alarmed or overwhelmed by the number of vulnerabilities uncovered during the audits. All 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 address 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. Make sure they are stored in accessible repositories and communicate around their publication. Set up a process to review and update them regularly at a certain frequency or when a specific event occurs.

Learn more:

- Awesome onboarding - http://bit.ly/2ws6OwE
- Rippling - http://bit.ly/2MXEqwE

✔ Ask questions and take notes during onboarding

Regardless of the maturity of the onboarding process at the 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 the security aspects during the onboarding. You can compile your observations within a discovery report.

✔ 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.

Learn more:

- 10 Tips to Reduce Common Vulnerabilities Exploited by Cybercriminals - http://bit.ly/2M6BFV9
- How to Prepare For Your Next Penetration Test - http://bit.ly/2NIL5AT
- 10 steps to managing a successful network penetration test - http://bit.ly/2wPtVBx

---

✔ 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 and can't by no means be considered as enough.

Learn more:

- Launching an Efficient and Cost-Effective Bug Bounty Program - http://bit.ly/2LEORAt
- Hackerone - http://bit.ly/2NAnKIv

✔ Structure and be the technical resource for the 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.

- CSA - Cloud Security Alliance - http://bit.ly/2C3nTDa

✔ Understand product development processes

As part of your exploration, you need to gather enough information from the key stakeholders in order to have a clear understanding of the product development processes (steps, key milestones, teams involved, governance structure...). It can be documentation or detailed oral explanations that should be written down. It will serve as a basis when you get to introduce security awareness and tasks within the processes.

✔ Be smart

As a security engineer your job is to improve the security of your new company. It's tempting to show off how much you know about security and cybersplain everyone how insecure their setup is. Don't just take your previous experiences and more mature companies as the go-to model. Understand what's at stake (risk management). It's easy to suffocate an agile startup with heavy security that does not scale well. Security Engineers operate inside a business and understanding the business before enforcing GovAgency-like security measures is key.

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. 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 the stakeholders

If it was not included in your onboarding documentation, ask for the list of the key stakeholders in the organization, whether developers, operations, leaders 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, of your role and their concerns.

✔ Do a security training for engineers and non-engineers

Liaise with HR or the training department to set up a targeted security training for all employees, whether engineers or not. The training should not be a list of instructions, rather an explanation as to why certain rules have to be put in place. You can include technical details but make them accessible for all skill levels. The training should be included in the onboarding process of the newcomers.

✔ 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 forget 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, laptops and external drives.

- Security begins with the reception desk - http://bit.ly/2CA87jA
- Ten Recommendations for Security Awareness Programs - http://bit.ly/2ws327f
- 7 elements of a successful security awareness program - http://bit.ly/2NUWYLe

---

✔ Meet with fellow security engineers from similar companies

It is a good practice to share and discuss with fellow professionals. As such, if you are not already a member of a professional group in your area, look for the local chapter of Information Security communities. You could also reach out directly to fellow security engineers, whether in same business line or not, to exchange ideas about your jobs and responsibilities or to discuss how they navigated being the first security engineer in their organization, if they were.

Learn more:

- Information Security Community (LinkedIn group) - http://bit.ly/2wSMPrS
- Information Systems Security Association (ISSA) - http://bit.ly/2M4yz4h

---

✔ 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 some websites on which you can get regular information.

Learn more:

- 4 Essential Steps to Protect Web Applications - http://bit.ly/2QfXVPY
- OWASP Top Ten Project - http://bit.ly/2POeRgg
- AppSec USA - http://bit.ly/2NQsn1b
- Down the Security Rabbithole - http://bit.ly/2wPx1p8

APPLICATION SECURITY

✔Add a security policy to the websites

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

Learn more:

- Open Source Security Page - http://bit.ly/2LFyPX9
- https://securitytxt.org - http://bit.ly/2Qc2xGP

✔Audit DNS settings

As more and more day-to-day business activities and revenue rely heavily on the DNS, it is important to check it as soon as possible and regularly ward.

Learn more:

- Eight reasons why you should conduct a DNS audit - http://bit.ly/2CnlXp8

✔Audit the application

Perform an audit of the applications, check the dependencies, and the user accounts.

Learn more:

- Awesome Pentest Cheat Sheets - http://bit.ly/2MaRXg4
- Use Sqreen during your audit to find and remediate issues faster - http://bit.ly/2MDSMTm
- Web Application Security Testing Cheat Sheet - http://bit.ly/2wRdfJE
- OWASP Top Ten Project - http://bit.ly/2POeRgg
- Auditing Applications, Part 1 - http://bit.ly/2wPMnLb

- Auditing Applications, Part 2 - http://bit.ly/2MWQPSx

✔ Enforce two-factor authentication

Wherever possible, make sure two-factor authentication (2FA) is enforced. It requires the user to provide a second piece of information on top of a password which adds strength to the login process.

Learn more:

- Duo Security - https://duo.sc/2LEODJu
- Auth0 - http://bit.ly/2wu0UM9
- What is two-factor authentication (2FA)? - http://bit.ly/2wPyk7x

✔ Ensure dependencies are secure

Include security in all steps of the product development process and not just at the testing phase. Security-minded developers check the dependencies for known bugs and vulnerabilities before using them and they make sure to keep updated when zero-days are found or patches are available.

Learn more:

- 13 tools for checking the security risk of open-source dependencies - http://bit.ly/2Q5O2nI
- Security alerts on Github - http://bit.ly/2wQLrpP
- Sqreen - http://bit.ly/2MDSMTm

✔Help engineering and business teams protect sensitive business logics

The attacks representing the most significant business risk for our organizations are often attacks targeting sensitive business functions of our applications. Work with business and engineering teams to identify the biggest threats and implement monitoring and protection solutions to automatically remediate these threats.
Integrate security automation into your app

✔Make sure everything is properly encrypted

When it comes to cryptography, don't use your own but use standards. Encrypt everything: 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.

Learn more:

- Let's Encrypt - http://bit.ly/2wvISsi
- Microsoft encryption - http://bit.ly/2MGo64g
- MacOs encryption - https://apple.co/2wqNM9K

✔Protect from intrusions and data breaches

Use tools like Sqreen to prevent data breaches, protect your customers, stop business logic attacks and get full visibility on your security.

✔Retrieve and audit the backups or set up new backups

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

✔Secure your emails with DMARC

Emails are usually the weak door for attacks, especially through phishing and spoofing. A single email can make serious damages. You can implement DMARC (Domain-based Message Authentication, Reporting and Conformance) to protect your users from fraudulent emails.

Learn more:

- DMARC - http://bit.ly/2oMwIHW
- How to Set Up and Implement DMARC Email Security - http://bit.ly/2oLL0sh
- Build Your DMARC Record in 15 Minutes - http://bit.ly/2wXMvZd
- OnDMARC - http://bit.ly/2MXuKTS

✔ 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

Learn more:

- Vault Project - http://bit.ly/2wu37Hu
- AWS CloudHSM - https://amzn.to/2wxp8Ex
- Tips for private key management - http://bit.ly/2wOsT9G
- An Introduction to Managing Secrets Safely with Version Control Systems - https://do.co/2Qbdd8A

✔ Think about centralized authentication

The benefits of centralized authentication for the users is having a single set of credentials for all their applications. From a security standpoint, it enables to handle only one account and avoids forgetting to disable an account during offboarding (and it saves time also during onboarding instead of creating an account in each application)

Learn more:

- Five Lessons We Learned on Our Way to Centralized Authentication - http://bit.ly/2Cz6ZMK
- Centralized Linux Authentication - https://do.co/2wR3Dzv

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. Setting up firewalls and limiting the number of password guesses are some of the measures that can be implemented to protect your servers, and consequently the applications.

Learn more:

- Sqreen - http://bit.ly/2MDSMTm
- ThreatStack - http://bit.ly/2wr8WVq
- 7 Security Measures to Protect Your Servers - https://do.co/2Qbd58R
- How To Protect SSH with Fail2Ban on Ubuntu 14.04 - https://do.co/2MV8eKt

✔ Start thinking about hardware protection

Security threats can also come from physical access to the hardware. Assess the risks for your company's hardware and plan accordingly.

Learn more:

- 10 physical security measures every organization should take - https://tek.io/2oLU6Fv

MONITORING

✔ Assess the assets information

As a first step, assess the availability and freshness of the assets information. Is there a list of the hardware? Is there a list of the applications used within the company? Is there an employee directory and a list of the users' accounts? Is there a list of the third-party providers and the contracts? When were these lists last updated? Employee directory might be the easiest to retrieve as personnel department should be able to provide up-to-date records with dates of joining and leaving the company. As for the other lists, you will probably have to build them or update them if they exist.

✔ Audit cloud providers

Know your cloud services! Security is the first concern when it comes to cloud computing. Examine the settings and SLAs of the cloud services, whether application, platform or infrastructure, and compare with what was agreed on in the contracts. Take note of the flaws in the contracts to renegotiate them if needed. Cloud 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.

Learn more:

- Security of SaaS Companies - http://bit.ly/2CqKx8v
- GDPR Tracker - http://bit.ly/2oMABws
- Audits and compliance requirements for cloud computing - http://bit.ly/2QbyWx8
- Securing the cloud with compliance auditing - http://bit.ly/2wNkwdO

✔ Build a security dashboard

Create a security dashboard to give you an overview of the security efforts. Avoid manual reporting, all the data should be automatically provided by the solutions used.

- The Top 10 Tips for Building an Effective Security Dashboard - http://bit.ly/2LZHLH3

✔ Evaluate third-party providers

Conduct thorough assessments of the third-party providers to make sure they are secure. Renegotiate the contracts to strengthen the responsibilities of the providers and the service levels required.

✔ Perform a first security audit

Design and perform a first security audit to understand the most critical security vulnerabilities. This first audit should be broad in scope but not too detailed as other more thorough audits will be performed for specific areas.

Learn more:

- How to Conduct an Internal Security Audit in Five Simple, Inexpensive Steps - http://bit.ly/2MQ60g5
- Prioritizing Your Security – Where Do You Begin? - http://bit.ly/2CsyAiL

✔ Protect against Denial of Service attacks

Denial of Service (DoS) attacks are attempts to affect the availability of the websites or applications to legitimate users. Distributed Denial of Service (DDoS) are larger scale attacks pursuing the same objective. These attacks can be devastating for a business. Thus taking actions to protect the systems and mitigate the effects of the attacks is key.

Learn more:

- AWS Shield - https://amzn.to/2M4aASE
- Four ways to defend against DDoS attacks - http://bit.ly/2wRdO6x

- DDoS protection, mitigation and defense: 7 essential tips - http://bit.ly/2CtvcV3
- Best DDoS protection of 2018 - http://bit.ly/2wSQbes
- Cloudflare - http://bit.ly/2C0sB4t

✔ Set up a centralized logging platform

Logs are the most precious assets to monitor the environment and to investigate a suspicious activity or a security breach. A centralized log platform enables to make the most out of the analytics capabilities and provides a view across all themes (applications, network, users, etc.)

Learn more:

- Logging Cheat Sheet - http://bit.ly/2NUIvPu
- What is log management and how to choose the right tools - http://bit.ly/2Q8SGkO
- Centralized Logging on AWS - https://amzn.to/2M4iOub
- Top 7 Success Factors for Setting Up Centralized Logging - http://bit.ly/2NSv4zn

---

✔ Update or build the list of applications

If you have been handed a list of the applications in use within the company, make sure it is up-to-date or take time to update the information about the major applications first and schedule to update the rest of the list comprehensively as soon as possible. If there is no application list, you should build it. Ask if the employees have (or had previously) admin rights to install software themselves on their computer and identify the shadow IT.

✔ 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 the 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.

Learn more:

- Mobile Device Management Best Practices - https://ibm.co/2wODEYG
- Guidelines for Managing the Security of Mobile Devices in the Enterprise - http://bit.ly/2QaAOpK

✔ Update or build the list of third-party providers

You will need to know every company or individual which 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 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.

www.sqreen.io