IT security
for your company

TestArmy

About **the author**

Dawid Bałut

Cyber Security Director at TestArmy

A seasoned penetration tester and bug hunter, who spent half a decade testing security of hundreds of companies, including big corporations such as Apple, Amazon and Facebook. Then decided to join the defensive side of the force and for the next 6 years worked as a Security Architect for Silicon Valley based startup.

These days he's building security systems, automating all security operations possible and coaching employees in the spirit of DevSecOps. In his spare time he shares his thoughts in social media and creates free educational materials on security management, empathetic leadership and business development.

About **TestArmy**

TestArmy is an elite and well organized testing special forces unit. Our field of expertise is testing security, functionality and performance of everything that can be tested, from banking apps to smart toothbrushes.

We have been helping companies from all over the globe keep their products secure and flawless for over 7 years.

Ensuring that your systems are safe and secure **isn’t easy, but it can be a bit simpler**

TestArmy

In contemporary security world, you are likely to hear about concepts such as penetration tests, bug bounty programs and vulnerability researches very often. You should be made aware, that although these solutions are great and hold their tremendous value at the right moment, they are not the most important, nor most cost-effective initiatives for most companies. Let’s put first things first. The main reason is that all of the aforementioned engagements focus on the last phase of Software Development Life Cycle, which is when the product is complete and ready.

The challenge origins from a fact that the cost of implementing changes - including security bug fixes - increases significantly with each stage of Software Development Life Cycle. If we start considering the penetration tests, but we haven’t had invested in securing earlier phases of SDLC, we’re putting ourselves into a situation, where ensuring high security standards may come with staggering costs.

Developers working with code focus on quick completion of their tasks to meet projects deadlines and deliver functionable software. Hurry in software development results in an increased number of security vulnerabilities introduced at all stages of software engineering. That’s where our testers can help by guarding product quality, so that developers can focus on the work that really matters. Developers can request help from our specialized testers anytime and either consult a problem or delegate testing tasks. With an access to the source code, our experts can also conduct tests of modules of any size and help programmers ship the software on time, yet without compromising its quality.

> ***General rule in effective security programs is that the earlier you start paying attention to security, the less you’ll need to pay in resources later, when there is a need to fix a vulnerability.***

Quality Assurance is **now much more than it used to be**

Tech giants have already figured it out, which is why they heavily invest in internal testing processes that go way beyond regular QA we used to see in the past. Functional bugs are costly because they can discourage users from using an app for a while, but it's security bugs where craziness jumps in and it can end up even with company's bankruptcy. Companies can't afford to have a security vulnerability in a publicly available product anymore. Let's take a look at some of the most popular factors that make companies invest in security:

1) A will to differentiate from competitors
2) Solid requirements stated by customers
3) Regulations mandated by local/global laws and governments
4) Being afraid of a costly data breach
5) Worry of becoming a target of security professionals who can uncover and disclose the real state of corporation's security

Let's take a look at these points, one at a time:

A will to differentiate from competitors

If you get yourself ahead of the curve, you can use that as a marketing tool and show your customers that along with your product, they're buying trust, highly reliable service and respect for confidentiality of their data. But it's not all about classic technical security measures such as how well is your SDLC protected.

If your product has a more user friendly implementation of security mechanisms, such as Two Factor Authentication, customers will be really happy about it. The decision makers know how low products adoption can get, if security features in a product offer bad UX. Customers invest in your platform to use it as a tool meant to benefit their business, and the benefit isn't that great if their employees are afraid of using your product.

Solid requirements stated by customers

In days when data extortion is such a lucrative business for online thieves, corporate customers want to feel comfortable with safety of your products and services. Customers expect vendors to provide safe products, so they can sleep well and not worry about their privacy. With corporate customers this is even more serious. There is not a single CEO that would like a fact of his company's financial records and patents leaking to the Internet and being made accessible to fraudsters and competition. If your product isn't safe enough, it'll be getting increasingly harder for you to sell such a product or service. Customers, especially those from the financial industry are very conscious and aware of security risks, so if you're going for big fish, high security standards are a must.

Regulations mandated by local/ global laws and governments

With GDPR being a great requirement, not a single business can afford negligence in security assurance. Costs and consequences are far too high to allow oneself to ignore the need of strict security policies and procedures. The sooner you start implementing security measures, the more likely it is that you'll avoid the penalties, which in some cases can put your whole business on hold.

Our experts can help you assess the risks associated with your data processing processes. Our Security Team performs GDPR audits in collaboration with the Legal Team to ensure that your practices meet the requirements of the new EU directive on personal data protection.

Implementation of procedures that are in line with the new regulations requires a thorough audit of the current situation in the company. Our Audit Team can help you implement mechanisms meant to protect your company from data leakages. We can also introduce you into the world of Incident Response procedures which can come invaluable in case of an actual data breach.

Being afraid of a costly data breach

Data breaches cost a lot. In the era of rising popularity of ransomware, the single entry point can have a devastating results on your infrastructure. Data extortion, ransomware, cryptomining software and malware which slows your network down - all these things can have direct and indirect negative effect on your business. If your servers work slower, it may result in those less patient customers leaving your website and going to buy the thing from the competition. Precisely speaking, most businesses can't afford to get breached. Especially the SMBs and startups that are still fighting for their reputation, can't let their customers down at the very beginning of establishing the brand's credibility and value.

In early stages of building business reputation, each single slightly shady situation may decide whether your business will hold on the market or collapse.

Worry of becoming a target of security professionals who can uncover and disclose the real state of corporation's security

Reputation matters a lot. Security community is great and there is a huge number of people who conduct vulnerability research and seek vulnerabilities in popular software. While not intended, disclosure of those findings can result in reputational losses, highly depending on how you handle the disclosure process. If you work with researchers well, you'll be put in good light, however if you don't behave well or you face a researcher who has very weak social skills, all cards can be turned against you. Vulnerability research and bug hunting is very popular these days, so it's better to invest in security early, rather than hope that your security gaps won't be discovered. Hope isn't a good business risk management strategy.

How mindset change can make your company safer

In many companies security is being perceived as a necessary evil, because it costs money. Everything is in details and mindset, and having a negative attitude to security investments, is not the right way to go about it. It's hard enough, so why make it even more cumbersome? When we talk about Returns of Investments of security engagements, we mean the indirect ROI which is avoidance of losses.

When you start looking at security from this perspective, as for something that can help you save plenty of money, it's a whole different story and your executive team will be more eager to spend money on infosec.

If you're a software company, security can boost your sales because customers nowadays have pretty good general awareness about security. It puts them in position to make demands about quality of your products.

By having confidence and being able to prove that your product is more secure than your competitors' one, you can sometimes win a deal just by that.

In some industries, security is a mission critical requirement and it's not the cost, features or usability that makes customer choose specific vendor. It's the assurance that customer's data is safer with you, a vendor that heavily invests in security to be in top of the game.

You invest in security to protect yourself against financial losses, and sometimes you can use it as leverage while competing for a customer.

How do you achieve better results with the same investments?

TestArmy

That's a huge challenge indeed. Security industry taught companies how to make investments, but hasn't really focused on efficiency of those investments. If you pick your battles smart, you can achieve much better security posture than your competition, so let's dig into this and see what could be done better, to achieve greater results at the same or even lower cost.

Simply hiring external penetration testers doesn't cut it anymore. Software engineering processes have changed significantly so using just penetration tests is not effective and basically every company is doing it, so it's hard to differentiate that way.

If you truly want to go an extra mile, if you want to win trust of your customers, you have to put in the work, because your competitors aren't that much behind. Lots of businesses these days are aware about the need for security investments, but most of them can't get it right.

Everything in business should be driven by proper risk analytics, but to effectively manage risks, you need to know the costs of remediations and all the alternative paths. Only with a wide context you can make a good judgment on your risk profile.

Security Assurance is expensive, but doesn't need to be THAT expensive.

TestArmy

You have probably heard about things such as penetration testing, vulnerability assessments and bug bounties. These things are all over the place and it's hard not to hear about them. But it doesn't mean you should go after these things, before there is a couple of other things that can have higher and long-term ROI for you.

Let's consider the most common phases of SDLC, which are planning, requirements analysis, design, development, testing, implementation and maintenance. Conventional penetration tests can be performed in the last three ones, namely during testing, implementation and maintenance.

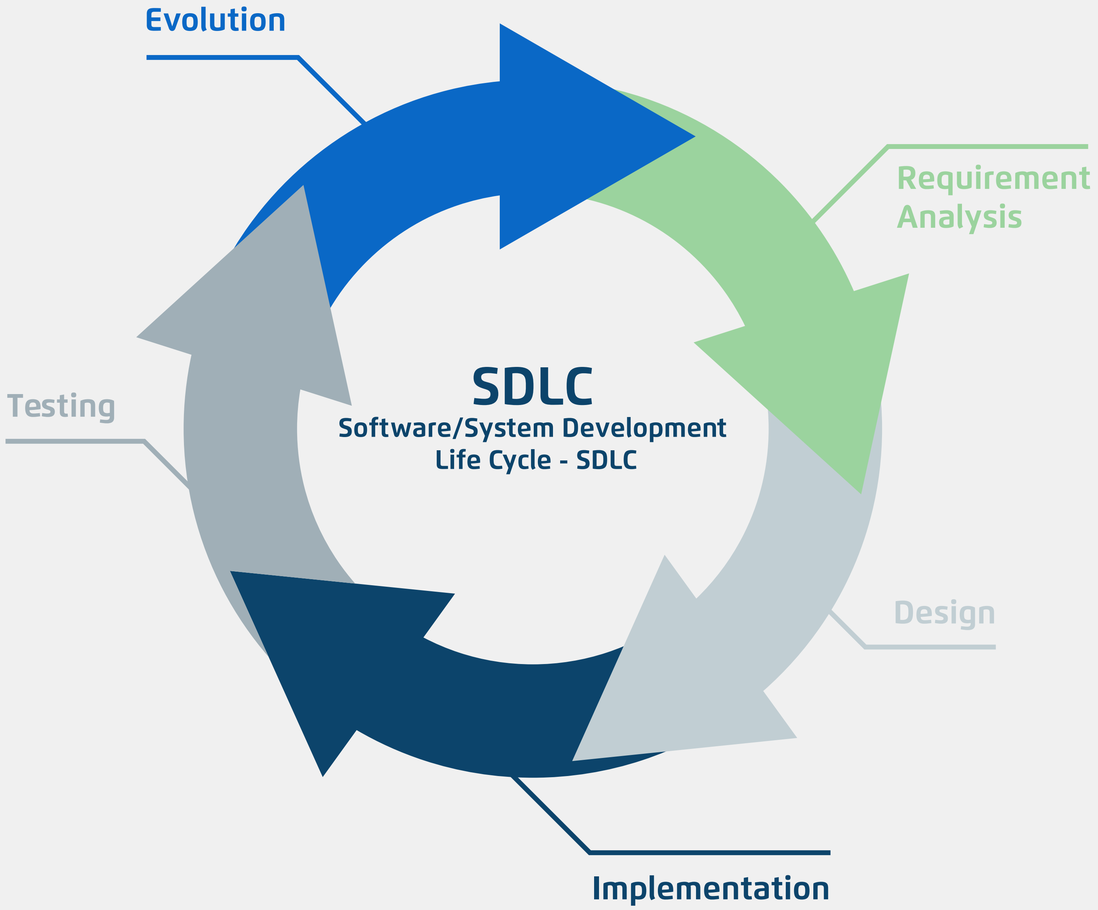
If you engage in security activities in the internal testing phase(5), you've already skipped 4 stages where you could identify flaws and fix them at a lower cost. Many companies actually hire pentesters to test products deployed in production, thus skipping 6 phases of SDLC.

Across all companies we've worked with, we notice following requirements:

- they need to have software built fast
- they need to have software tested and stable
- they need to have product in front of customers as soon as possible products must be developed even when engineers are tired and distracted.

> ***Educating software engineers, product owners and internal QA engineers will allow them to create safer products from the very first stages of SDLC***

To address the problem at its core, it's recommended to invest in the indispensable at all organisations - which are the people. Educating software engineers, product owners and internal QA engineers will allow them to create safer products from the very first stages of SDLC. If you have security-conscious engineers on your team, they can identify flaws in products design and business logic, decreasing amount of bugs that would need to be fixed in the future.We have built a security awareness framework, which you can use to help your engineers do a better job. Every one of us is already overloaded with important tasks and programmers don't have enough time to learn complex subjects such as security on their own. Investing in professional trainers and training materials will help you decrease the costs of software engineering in the long run. By shifting the developers' mindset a bit, you won't be slowing down the software release schedule, because engineers will simply do things right using solutions stored in their brains.



Security can be agile too!

TestArmy

Security for decades used to be a thing that slows everyone down, increases the cost and is burdensome to maintain. We used to produce software in the waterfall model, and we treated security assurance exactly the same way. Days of waterfall software development are long gone for many companies. Security processes should and can follow. We have all technical means to make the change, but we're missing the mindset, experience and will to do it.

Moving security to the left of SDLC makes the efforts much more effective. If we instill the security practices in all phases of SLDC, but we give ourselves more time to improve.

The core problem with security assurance is that we used to do most of it manually, and looking from that perspective, indeed it's hard to figure out how we could make manual security quality assurance more agile. We must heavily automate our processes, to ensure that all code is secured before it goes live, and we must automate in a smart way. It's not enough to download automated scanners and point them all at the application expecting actionable results. You need to learn how your application works and which external tools will come handy for your very specific technology stack. You need to instruct those tools how to connect to your application and how to perform meaningful tests.

Then you need to take the output from those tools and distinguish what's good and what doesn't make sense. You need all these things because you don't want to flood your developers with noise that could decrease their productiveness.

There are cost-effective tools for supporting your engineers during the design phase. There are tools supporting developers while writing code and there are tools that will help your IT OPS deploy the product safely.

Once you have everything in place and running, cost of maintenance is very low, and going further, you benefit from having less bugs in your code, that would require expensive patches or redesigns.

Get step-by-step guidance through security processes implementation.

Contact our consultant

Penetration tests and offensive security

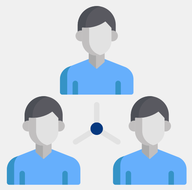
But what if you already have a finished application or have all those great Secure SDLC processes in place? At a certain point, final penetration testing is inevitable and can provide you with great results.

Penetration testers are testers specialized in security tests, but it's not only the technical knowledge that differentiates them. Penetration testers have a certain mindset that allows them to operate like hackers and find security flaws in your systems that could've been missed by QA Testers and software engineers. Programmers are taught and required to think like builders and decent Internet users who want to do no harm to anyone. Penetration testers on the other hand have been operating in a more offensive mindset for years, which wired their brains in a way that allows them to find novel ways to exploit holes in your systems.

1. Penetration Tests and Red Teaming

2. Infrastracture and Network Tests

3. Social Engineering Tests.



4. Blue Teaming

External penetration testers can test your systems top to bottom, providing you procedural guidelines on what issues still reside in your applications or infrastructure. Competent penetration testing team can identify gaps and provide you with detailed information on what could be done better, so you don't face the same issues in the future.

By engaging with right penetration testers, you can use their expertise in order to improve your SDLC even more. There is a lot of benefits of using penetration testing services to ensure quality of your software, however you should be aware that it's icing on the cake and you really need that cake first. Otherwise you're setting yourself up for frustrations and waste of money, because first things come first and trying to go around the recommendations can cost you a lot of resources.

What are the types of security testing?

Security audits come in many flavors, although the ultimate goal is always to identify and remediate security gaps in client's systems.
We're able to assess the safety of IT systems such as - but not limited to - web applications, by employing various forms of engagements including vulnerability assessments, source code and configurations reviews.

Penetration Tests and Red Teaming (Offensive Security Testing) are more sophisticated types of security testing. These are meant to simulate a real hacking attempt, where we try to behave like a hacker and break into your IT systems. Then we point out the holes for remediation, so that after you fix the identified issues, actual malicious attackers will have a harder time trying to penetrate your security. We're competent in conducting white box, gray box and black box security tests.

During Red Teaming engagements, we will also interface with your internal teams to help you build more robust infrastructure and better monitoring capabilities. Thanks to lessons learnt during our tests, you'll be able to catch attackers sooner and lock them out of your system before they cause a real damage.

Testing security of your network infrastructure is meant to improve the whole CIA triad of your organisation. Our tests aim to improve Confidentiality, Availability and Integrity of your systems and data.

Both external and internal infrastructure testing will guide you on the path of improving network safety and performance. The tests are carried out by our experts remotely or at the headquarters of the audited organization. Through the verification of laptops, wi-fi networks, wi-fi routers, printers, webcams, employees' smartphones, other network devices in the corporate LAN we can assess the security risks and advise on pragmatic improvements. All of our activities are then summarized in a detailed report consisting of identified vulnerabilities and list of suggested remediation steps.

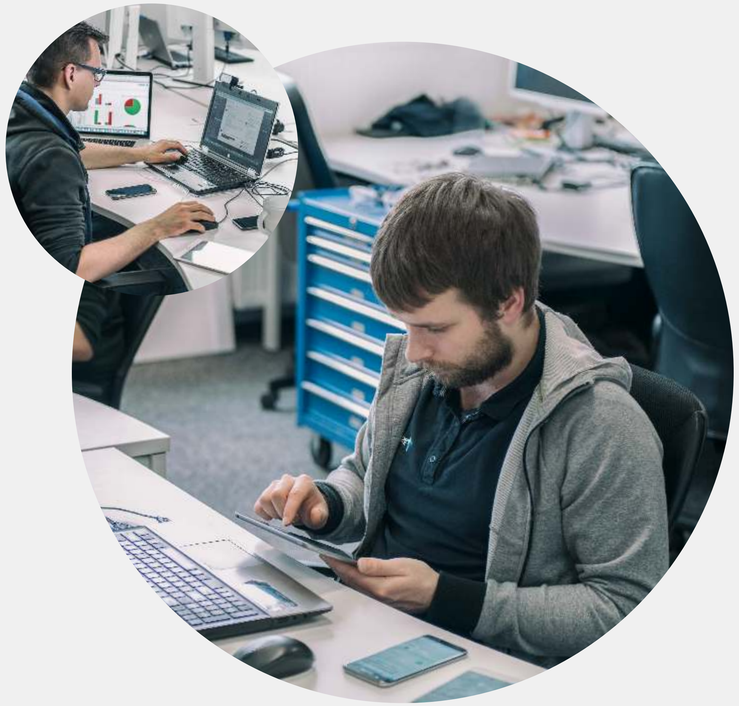
The most vulnerable element is not technology

It’s the processes, policies and our security awareness trainings that make us especially prone to attacks. If a company does not spend enough resources on coaching the staff across all of the offices on importance of high security hygiene, they can fall to social engineering attacks.

Social engineering attacks aren’t a topic as known and popular, as technical penetration tests. Which is a shame, because real hackers use social engineering a lot to be more efficiently and it works. Why would you waste hundreds of hours pentesting an application if you can call the front desk impersonating the IT Admin and request the office manager to forward sensitive documents to provided email address. Most people are empathetic creatures who’re easy to be abused by exploiting our compassion, sympathy or fear. Skilled social engineer with just a single phone call, can extort personally identifiable information or credentials that can be used to break into the system.

Social engineering tests aim to exploit the human element in the IT systems by manipulating an empathetic victim into performing a malicious activity against their company. Such activity may include revealing sensitive corporate data, enabling external access to restricted resources or sharing personal credentials with attackers. We perform such simulations, to check staff’s exposure to social engineering attacks by closely observing their attitude and behavior.

Our experts implement advanced attack scenarios in order to extort sensitive information thus discovering weak spots in company’s security posture.



The most vulnerable element is not technology

TestArmy

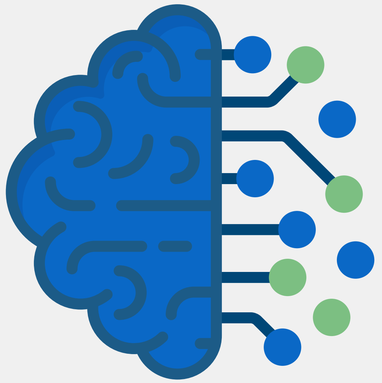
It's the processes, policies and our security awareness trainings that make us especially prone to attacks. If a company does not spend enough resources on coaching the staff across all of the offices on importance of high security hygiene, they can fall to social engineering attacks.

Social engineering attacks aren't a topic as known and popular, as technical penetration tests. Which is a shame, because real hackers use social engineering a lot to be more efficiently and it works. Why would you waste hundreds of hours pentesting an application if you can call the front desk impersonating the IT Admin and request the office manager to forward sensitive documents to provided email address.

Most people are empathetic creatures who're easy to be abused by exploiting our compassion, sympathy or fear. Skilled social engineer with just a single phone call, can extort personally identifiable information or credentials that can be used to break into the system.

Social engineering tests aim to exploit the human element in the IT systems by manipulating an empathetic victim into performing a malicious activity against their company. Such activity may include revealing sensitive corporate data, enabling external access to restricted resources or sharing personal credentials with attackers. We perform such simulations, to check staff's exposure to social engineering attacks by closely observing their attitude and behavior.

Our experts implement advanced attack scenarios in order to extort sensitive information thus discovering weak spots in company's security posture.



Increase you employees' awareness and your company's security with TestArmy

Check more

But what if?

In dynamically changing cyber security world, you need to be always looking into the future with a dose of pessimism. You never know when you are going to be attacked, but you must be prepared for what to do when such an incident occurs.

Most companies do not even consider a data recovery situation and do not test their protocols properly. To get ahead of the game, it takes you being more practical than others and while working on the best, expecting the worst.

To minimize the costs of a data breach, you need to have a well prepared strategy, which involves effective communication and data recovery tactics. Most people think about creating and testing the backups but there is much more you can do to contain the devastating results of a breach. We are talking about practical procedures meant to be used as a way of minimizing the reputation losses, financial losses and losses in customers. You must have a plan ready, that considers multiple facets of your organisation.

It happened

Dealing with the breach is stressful itself and you do not want to bother with additional technical activities around threat analysis and general forencisc management.

Our team of IT Forensics Experts can help you prepare for, and handle the security incidents if such occured. The Blue Teaming Unit can analyze the threats, investigate the breach and respond accordingly to minimize the business costs of an incident.

Competently executed incident response is critical in ensuring continuous business operations and includes aspects such as maintaining systems stability and retaining positive public relations. A security breach can affect any company, but it's the incident response phase that determines the consequences of a breach.

Any questions?

Call Jason!

Contact

Jason Burton
Business Consultant

+48 505 051 495
jason.burton@testarmy.com

TestArmy Group S.A.

+48 600 993 557
contact@testarmy.com
www.testarmy.com