SOVTECH™

Business Software. Sorted.

# Best Practices For Protecting Your Software Development From Cyberattacks

SOVTECH™
Business Software. Sorted.

# What are cyber threats or attacks?

A cyber attack is an intentional exploitation of computer systems or networks using malicious code. The purpose is to compromise data, steal information, or hold data hostage. The damage caused by cyber-attacks can be severe, leading to financial losses, compromised sensitive information, and potential bankruptcy for businesses. Additionally, customer trust and relations can be damaged, resulting in a decrease in confidence in the affected organization. Competitors can also capitalize on these vulnerabilities by implementing strong cyber attack defenses to prevent similar incidents.

## QUICK READ
## KEY INSIGHTS

A custom app allows you to create an interface that is tailored to your target audience, ensuring a seamless and enjoyable experience.

A unique app helps you stand out from the competition and attract more customers. In a world where off-the-shelf solutions are abundant, a custom mobile app acts as a distinctive and exclusive suit that sets you apart in the crowd

A well-designed custom app can significantly enhance your brand's reputation and credibility in the market. A reliable app will demonstrate your commitment to delivering high-quality products and services.

## What does this mean for the African continent?

The rapid development and digitization of businesses in Africa have increased the vulnerability to cyber threats. Despite the benefits, there has been a significant rise in cyber-attacks, with countries like South Africa, Kenya, and Morocco experiencing millions of threat detections. The expansion of digital services has widened the attack surface, posing challenges for African enterprises. Alarmingly, 90% of African businesses lack sufficient cybersecurity protocols. African leaders acknowledge the importance of prioritizing cyber attack prevention, and it is crucial for businesses and organizations to establish cybersecurity measures as more people come online.

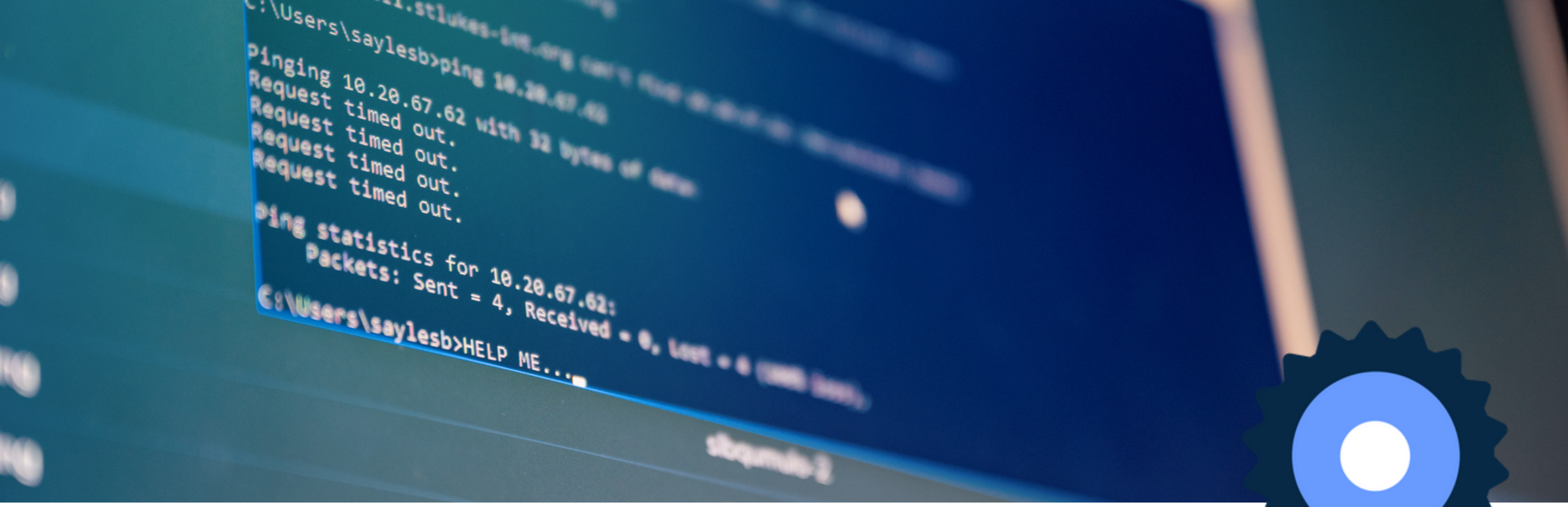
## Ways in which to protect your code

### Employee training for software developers

- The passage emphasizes the importance of cybersecurity in the context of digitized businesses and organizations, specifically focusing on the code they run on. Training employees on cyber attack prevention and informing them about current threats is crucial in protecting against cyber-attacks and data breaches. Secure coding practices, such as input data validation and proper authentication and password management, help mitigate vulnerabilities in the code.

### Keep your dependencies up to date

- Keeping dependencies up to date is another key aspect of securing software, as it prevents known vulnerabilities and provides access to new features and bug fixes. While there are risks associated with updating dependencies, the benefits include vulnerability prevention, access to new features, and protection against zero-day vulnerabilities. Regularly updating dependencies allows for quick and effective responses to security alerts.



```
C:\Users\saylesb>ping 10.20.67.62
Pinging 10.20.67.62 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.20.67.62:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\saylesb>HELP ME...
```

### Use encryption

- Encryption is emphasized as a crucial tool for software protection against cyber attacks. It converts text into secure messages, only accessible with the decryption key. Encryption safeguards data in transit, at rest, and in use, preventing interception and unauthorized access. The use of public and private keys, as well as symmetric and asymmetric encryption, is explained. Implementing encryption at different software levels is recommended, and it plays a vital role in combating evolving cyber threats and enhancing software security in the digital landscape.

### Implement secure authentication and authorisation

- Authentication and authorisation are discussed as vital aspects of identity and access management (IAM) in cybersecurity. Authentication verifies user identity through methods like usernames and passwords, while authorization grants access based on verified identity. IAM ensures appropriate access to resources for authorized users. Implementing multi-factor authentication (MFA) is recommended to enhance security against attacks like phishing. MFA requires multiple forms of evidence for access. IAM solutions support authentication and authorization, enabling control over access to applications, data sources, and development environments using factors such as passwords, mobile devices, biometrics, and location.

### Protect sensitive data

- Regular code reviews are crucial for software protection and reliability. They identify vulnerabilities and optimize code. Conducting regular reviews improves quality, security, and efficiency. Best practices include understanding the code, using automation tools, following a consistent process, and providing constructive feedback. Benefits include improved quality, enhanced security, increased efficiency, better collaboration, and learning opportunities.

### Regularly back up your code

- Regularly backing up software code is vital to defend against cyber attacks and data loss. Backups mitigate ransomware, insider threats, unauthorized access, and physical damage. They enable quick recovery, prevent losses, and protect intellectual property. Backups detect unauthorized changes and ensure code integrity. Using tailored backup strategies enhances software security against evolving threats.

### Implement proper error handling

- Improper error handling in software poses security risks by exposing sensitive details or causing system crashes. Proper error handling counters human mistakes and obstacles, handling feasible inputs and producing simple error messages. Best practices include logging and monitoring errors, secure error messages, input validation, structured exception handling, and thorough testing. Addressing error handling enhances security and reduces vulnerabilities in production.

### Employ a strong firewall and intrusion detection system (IDS)

- Firewalls and intrusion detection systems (IDS) are essential for network security. Firewalls control traffic based on rules, while IDS monitors for suspicious activity. Configuring the right system, updating regularly, and using VPNs and NAT enhances security.

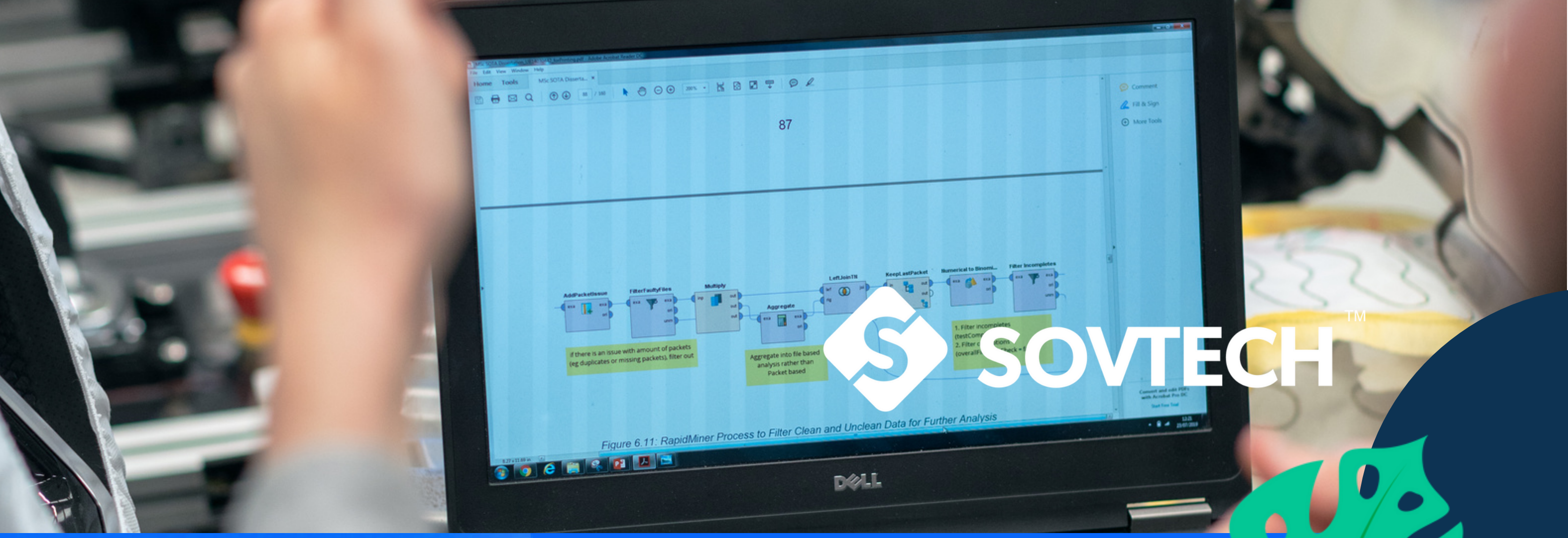
### Implement a bug bounty program

- Bug bounty programs allow ethical hackers to find security flaws in software by exploiting vulnerabilities. Benefits include cost-effectiveness and access to highly skilled individuals for rigorous testing. However, challenges include potential expenses and management complexity. These programs are effective for testing security protocols and providing reassurance to both organizations and customers. Regular deployment is recommended to maintain the system and site security.

# In Conclusion

Time and again as technology has evolved and scaled, many people have seen opportunities for growth and positive change. So too do other people see opportunities for their malicious intentions and selfish gain. More and more of our daily lives are conducted online and that'll only continue to grow. Personal information, intellectual property, and matters of high confidentiality are just a few examples of why concealing and protecting your systems is paramount.

Investing in cyber security is a non-negotiable for any business or organisation that uses software and code. It is the foundation to which everything else operates as it should because if it isn't there, the potential downfalls are disastrous. And those chances should not be taken, especially if you look to remain competitive in the online sector. It is one of the few investments where the returns will far outweigh its cost and will continue to compound as you go along.


87
Figure 6.11: RapidMiner Process to Filter Clean and Unclean Data for Further Analysis

# Working With SovTech

Working with ***SovTech*** offers the benefit of a commitment to continuous improvement. This means continually improving processes and systems to provide the highest level of service and support. This includes regular training and skills development for staff as well as sharing best practices and industry insights with clients.

***SovTech's*** staff augmentation services are flexible to meet clients' changing needs. Businesses can easily increase or decrease software team size for each project's needs. Working with ***SovTech*** provides access to experienced software developers and engineers to achieve development objectives.