Future Processing

SDL – **Security Development Lifecycle**

Ensure protection throughout the entire lifecycle of a development project. Leverage a comprehensive process integrating essential security practices into your solution from the initial idea to deployment.

www.future-processing.com

What you get:

- An end-to-end process integrating the cybersecurity best practices and tools into every stage of your solution's development
- Security as an integral part of your development process

As a result, you can:

- Ensure your solution's safety by managing and mitigating potential security risks
- Prevent cyberattacks and minimise potential system vulnerabilities
- Operate proactively rather than reactively regarding the cybersecurity of your solution

Benefits for your business:

- You will save costs thanks to implementing security early on in the process
- You will increase your customers' trust
- You will create and develop secure, stable, and efficient products

You should know:

- SDL (Security Development Lifecycle) encompasses the entire software development process
- Our security experts are involved in requirements gathering, solution design, development, and application deployment
- We support you in defining security requirements and provide guidance and support in implementing security solutions
- The security status of the developed solution is continuously monitored through both automated and manual tests

How we work:

- Our security experts rely on, but are not limited to, guidelines derived from the Microsoft Security Development Lifecycle
- We use modern software that enables threat modeling, automated static code analysis including external dependencies, as well as dynamic application security analysis

SDL practices we follow:

- Provide Training
- Perform Threat Modeling
- Define Metrics and Compliance Reporting
- Perform Dynamic Analysis Security Testing (DAST)
- Establish Design Requirements
- Desine and Use Cryptography Standards
- Use Approved Tools
- Perform Penetration Testing
- Define Security Requirements
- Manage the Security Risk of Using Third-Party Components
- Perform Static Analysis Security Testing (SAST)
- Establish s Standard Incident Response Process

Future Processing

Webapp **pentesting**

Protect your company by identifying security weaknesses and vulnerabilities within your web apps and minimise the risk of data breaches.

www.future-processing.com

What you get:

- A thorough assessment of security vulnerabilities within web applications
- A comprehensive report outlining the vulnerabilities and weaknesses identified during the assessment
- Easy to follow remedies on how to fix issues and vulnerabilities found in your application

As a result, you can:

- Identify security vulnerabilities and weaknesses within a web application
- Improve application security by identifying and addressing vulnerabilities that could be exploited by attackers
- Stay compliant with regulations related to data privacy and security
- Protect the reputation of your organisation and demonstrate your commitment to security issues
- Reduce financial risks linked to security breaches
- Meet regulatory requirements related to data privacy and security to avoid potential penalties

Benefits for your business:

- Enhanced security achieved by identifying and addressing potential vulnerabilities in the web applications significantly reduces risk of cyber attacks
- By proactively identifying security vulnerabilities you can address them before they lead to costly security incidents, which in result reduces the overall cost of security and prevent potential financial losses
- Compliance with industry regulations and standards related to data privacy and security reduces the risk of regulatory penalties and legal fees
- Web application security assessment allows to identify and prioritise potential security risks, meaning you can allocate your resources effectively and manage security risks more efficiently
- Access to security experts with specialised knowledge and experience in identifying and addressing security vulnerabilities in web applications means your web applications get the highest level of attention they deserve.

You should know:

- If you choose webapp pretesting services, you will get a detailed report on the vulnerabilities found, together with easy to follow, specific remedies on how to fix issues to improve the safety of your product
- Webapp penetration testing ensures verification of the safety of your product by the best experts, experienced not only in conducting the tests but also in developing safe apps, meaning they understand the problems from different angles
- When undertaking webapp penetration testing we act according to the best quality standards and use a variety of methods to better understand the hidden vulnerabilities of your application

The way we do it

The methodology of a web application security assessment involves seven stages:

1. Planning and scoping
2. Reconnaissance
3. Vulnerability scanning
4. Manual testing
5. Analysis and reporting
6. Remediation
7. Validation

Future Processing

Threat **modeling**

Identify risks and potential vulnerabilities in your system to prevent threats and increase your system's security.

www.future-processing.com

What you get:

- A thorough assessment of your system including identification and categorization of the threats it may face
- An assessment of identified risks together with a clear indication of whether they should be accepted, eliminated or mitigated
- An evaluation of the model together with a follow-up plan

As a result, you can:

- Increase the security of your system by identifying potential security threats before they are exploited by attackers
- Protect your organization's assets by identifying and mitigating the risks
- Ensure your products' and company's compliance with regulatory requirements
- Promote collaboration between security and development teams
- Improve the safety of your products and of data they use
- Stay ahead of the ever-evolving threat landscape

You should know:

- If you choose threat modeling, you will get a thorough picture of the safety of your product from the very beginning of its development process
- Threat modeling ensures verification of the safety of your systems by the best experts, experienced not only in conducting such tests but also in developing safe web products, which means they have a clear understanding of many issues they may face
- When working on threat modeling, we act according to the best quality standards and use all our experience to better understand the hidden vulnerabilities of your system.

Benefits for your business:

- The improved safety of your system means lower risk of security breaches which are costly, both in terms of money and reputation
- Threat modeling allows for identifying design flaws at early stages of development, making the process more cost and time-effective
- Compliance with requirements such as GDPR and PCI-DSS means increased reputation of your company which is noticed both by regulatory bodies and by your customers.

The way we do it

At a high level, our threat modeling service involves four stages:

1. Defining the scope
2. Identification and categorisation of threats
3. Assessment of identified risks
4. Evaluation of the model

Future Processing

Security requirements gathering

Identify potential risks and vulnerabilities that may affect the security of your system and address them.

What you get:

- A report containing the results of security requirements gathering with a list of found vulnerabilities
- Clearly presented information on the impact of findings on your business and the likelihood of the vulnerabilities being exploited
- Easy to follow remedies on how to address the vulnerabilities found in the system
- A plan of action

As a result, you can:

- Increase the security of your system or network
- Identify potential risks and vulnerabilities that may affect the security of your system
- Take steps to address the issues to increase the security of your system or network
- Stay ahead of the ever-evolving threat landscape
- Protect your company's reputation by taking care of its security posture
- Ensure your company adheres to industry standards and regulations

You should know:

- You will get a detailed report on the vulnerabilities found, together with easy to follow, specific remedies on how to fix issues to improve the safety of your network
- Security requirement gathering ensures verification of the safety of your network by the best experts, experienced not only in conducting the tests but also in more hands-on development work
- When undertaking security requirements gathering, we act according to the best quality standards

Benefits for your business:

- Thanks to expert identification of threats and vulnerabilities you will achieve improved, comprehensive security of your system or network
- Your adherence to industry standards and regulations guarantees regulatory compliance and increased stakeholder confidence.
- Early identification of requirements prevents costly reworks and in the long term means savings
- Enhanced risk management means early risk mitigating that protects your assets and reputation

The way we do it

Our security requirements gathering service involves five stages:

1. Scope definition
2. Information gathering
3. Stakeholder interviews
4. Security requirement identification
5. Preparing a comprehensive report detailing the vulnerabilities found

Future Processing

Security architecture review

Assess the security of your system’s architecture to identify potential security risks and vulnerabilities and protect your sensitive assets.

www.future-processing.com

What you get:

- A review of your system's overall architecture allowing to identify potential security risks and vulnerabilities
- Clearly presented information on the impact of findings on your business, which allow to proactively address the issues
- Improved security posture throughout your organisation

As a result, you can:

- Identify security risks within your system architecture
- Proactively address the issues and reduce the likelihood of security incidents
- Be compliant with regulatory standards to avoid penalties and reputational damage
- Improve your security posture to better protect your systems and data against cybercriminals
- Ensure business continuity by identifying and mitigating potential risks to the system's availability and resilience

You should know:

- By choosing security architecture review you will get a detailed report on the vulnerabilities and weaknesses of the system together with information on how to address them to improve your system's safety.
- Security architecture review involves working with SAS and DevOps teams to get a holistic picture of the quality of your system, which ensures the process is thorough and effective
- Your system's architecture will be reviewed by people who are not just auditors, but also engineers, meaning they understand the problems also from the purely technical point of view.

Benefits for your business:

- The improved safety of your system's architecture achieved by knowing its vulnerabilities, which means better protection against cybercriminals and improved security posture
- Compliance with the most important regulatory frameworks and standards which has a massive impact on the company's reputation and allows avoiding legal and financial penalties
- Constant continuity of business achieved by identifying potential risks to system's availability and minimising the impact of security incidents
- Third party assurance meaning your stakeholders such as customers, partners and suppliers know you implemented adequate security measures to protect their data and system, which has a massive impact on the reputation of your company

The way we do it

Our security review of the system's architecture involves evaluating the following aspects:

1. Architecture Design
2. Implementation
3. Configuration Management
4. Operations
5. Third-Party Dependencies

Future Processing

OSINT

(Open-Source Intelligence)

Gain insights on individuals, organisations, market trends and potential risks to make informed, effective business decisions.

www.future-processing.com

What you get:

- A detailed report including information collected, the analysis of the findings and suggestions for actions to minimise risks and increase security
- Clearly presented information on the impact of findings on your business
- Real-time insights and information on current events and market trends, important for making informed decisions

As a result, you can:

- Improve risk management by identifying potential risks and threats and taking proactive measure to mitigate them
- Assess vulnerabilities in your network or system to prevent cyberattacks
- Improve your incident response by gathering information on an ongoing cyberattack
- Identify potential fraud or financial crimes by monitoring social media and other sources for info on fraudulent activities
- Conduct thorough due diligence on potential acquisition targets by gathering information on their financial history, legal status and reputation

You should know:

- With our OSINT service you get valuable insights and information allowing you to achieve your goals, improve your operations and make informed decisions
- The goals you can achieve with OSINT service depend on your specific needs and objectives
- When undertaking OSINT service, we act according to the best quality standards and use a variety of methods to deliver information you are after.

Benefits for your business:

- OSINT is less expensive than other intelligence-gathering methods, allowing for better cost-effectiveness of your activities
- By identifying potential threats, vulnerabilities, and incidents before they escalate into more serious problems you can improve your organisation's security and risk management
- By gathering information from multiple sources, you get a comprehensive view of the acquisition, meaning more informed decisions
- With OSINT you get real-time insights and information on current events, market trends, and social media sentiment
- By gathering information from multiple sources and analysing it for patterns and trends you get a comprehensive view of a particular topic, issue, or individual.

The way we do it

Our OSINT testing service involves five stages:

1. Gathering information
2. Analysing information
3. Risk assessment
4. Reporting and presenting results
5. Implementation of actions

Future Processing

Mobile **pentesting**

Identify vulnerabilities and security weaknesses in your mobile applications and devices to increase their safety and protect them against cybercriminals.

www.future-processing.com

What you get:

- A report containing assessment results with a clear list of found vulnerabilities that can be exploited by cybercriminals
- Clearly presented information on the impact of findings on your business and the likelihood of the vulnerabilities being exploited
- Easy to follow remedies on how to fix issues and vulnerabilities found in your application
- A gap analysis against the industry best practices

As a result, you can:

- Increase the security of your mobile application and devices
- Prevent unauthorized access to sensitive information your mobile apps may contain
- Identify the weak points in your systems and take steps to mitigate them
- Improve the safety of your products by offering better user data protection
- Stay ahead of the ever-evolving threat landscape
- Protect your company's reputation by delivering secure and reliable products
- Ensure your products and company's compliance with regulatory requirements

You should know:

- If you choose mobile pretesting services, you will get a detailed report on the vulnerabilities found, together with easy to follow, specific remedies on how to fix issues to improve the safety of your product
- Mobile penetration testing ensures verification of the safety of your product by the best experts, experienced not only in conducting the tests but also in developing safe apps, meaning they understand the problems from different angles
- When undertaking mobile penetration testing, we act according to the best quality standards and use a variety of methods such as Black Box testing to simulate hacker activities in order to better understand the hidden vulnerabilities of your application

Benefits for your business:

- The improved safety of your mobile apps which means better protection against cybercriminals
- The higher user satisfaction linked to the increased safety of their data processed by your products which means clients will be more loyal to your product and will recommend it further
- Better protection means less risk linked to cyberattacks which cost both money and reputation

The way we do it

Our mobile pentesting usually involves six stages:

1. Planning and preparation
2. Reconnaissance
3. Threat Modeling
4. Vulnerability Assessment
5. Exploitation
6. Reporting
   See an exemplary report fragment on the right

5.2. [EX-2] MOBILE: BACKUP FOR MOBILE APPLICATION

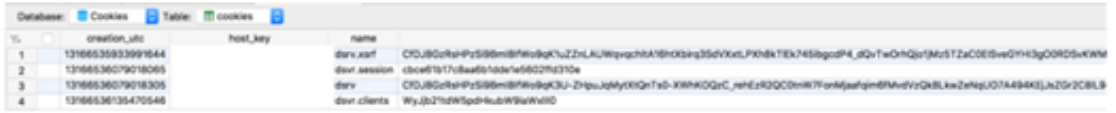
5.2.1. DESCRIPTION

Application Data can be Backed up - **[android:allowBackup]** flag is missing. This might allow to retrieve session tokens from application backup data:

Example of data found in Android 4.4.2 (LG V490) – JWT access token for application API (found using **cat com.application/r/app_webview/Cache/* |grep --text Silent** run against backup):

```
HTTP/1.1 302 FoundDate: Mon, 26 Mar 2018 06:16:28 GMTLocation:
https://xxx/Account/Silent#id_token=TOKEN
```

Example of data found in backup for Android 7 (Nexus device) – SSO session cookies stored in web_view cookie storage (xxx/r/app_webview):



5.2.2. IMPACT

Security Risk:	Medium		
Exploitability:	Low	**Impact:**	High

To exploit this issue attacker would need physical access to unlocked phone or to offline backup file.

Depending on Android version the following data might be available in backup (even after a user logs out from the application).

- Session tokens for SSO
- JWT tokens used to connect to API

Please note: Patients' data cached in the application is encrypted using secure method and cannot be extracted from backup. However, if session token is extracted, attacker might be able to retrieve this data directly from API.

Impact of this error increases the fact that temporary application data is not removed after explicit logout.

5.2.3. MITIGATION

Explicitly disable Android backup capability by setting **[android:allowBackup]** flag to false.

5.2.4. REFERENCES

- Mobile Top 10 2016-M2-Insecure Data Storage
- Android application settings

Future Processing

Infrastructure **pentesting**

Identify vulnerabilities and weaknesses in your organisation’s infrastructure and protect it against cybercriminals by simulating a real-world attack.

www.future-processing.com

What you get:

- A final report containing identified vulnerabilities and recommendations for remediation
- A thorough assessment of the effectiveness of your organisation's security and access controls
- Improved incident response
- Improved cybersecurity awareness across the whole organisation

As a result, you can:

- Increase the security of your infrastructure, including networks, applications and systems
- Understand your organisation's security risks and prioritise remediation efforts
- Assess the effectiveness of your organisation's security controls such as firewalls, IDS/IPS, DLP
- Ensure your products' and company's compliance with regulatory requirements
- Reduce the risk of a security breach by identifying and addressing vulnerabilities
- Improve your incident response capabilities by identifying gaps in your response plan and implementing recommendations for improvement

You should know:

- If you choose infrastructure pentesting services, you will get a detailed report on the vulnerabilities found, together with easy-to-follow recommendations for remediation
- Infrastructure penetration testing ensures verification of the safety of your products is conducted by the most experienced experts
- When undertaking infrastructure penetration testing, we act according to the best quality standards and use a variety of methods to simulate a real-life hacker activities in order to better understand the hidden vulnerabilities of your application

Benefits for your business:

- Valuable insights into security posture help make informed decisions and adjust your security strategy
- Identifying and prioritising vulnerabilities help optimize security spending and in the long term saves time and money
- Infrastructure penetration testing can be an essential component of a comprehensive compliance strategy, helping to meet regulatory requirements and avoid potential penalties
- Regular infrastructure penetration testing allows to stay ahead of evolving threats and to maintain a strong security posture
- Identification of potential gaps in security controls allows to proactively address vulnerabilities and reduce the risk of a security breach

The way we do it

Our infrastructure pentesting usually involves seven stages:

1. Defining the scope
2. Reconnaissance
3. Vulnerability scanning
4. Exploitation
5. Privilege escalation
6. Post-exploitation
7. Preparing a comprehensive report detailing the vulnerabilities found and our recommendations