IstroSec

Data Sheet

Offensive Security

As part of the comprehensive provision of an adequate level of security, it is necessary to reflect on new threats, verify the complexity and systematicity of implemented security measures, as well as detect the level of resilience of the organization to threats and attacks relevant to the organization.

We provide the following offensive security services:

- Vulnerability scan
- Vulnerability assessment
- Penetration test
- Red teaming
- Purple teaming

Vulnerability assessment

As part of vulnerability assessment, experts from **Istro**Sec perform vulnerability scans using automated tools (commercially available as well as self-developed for this purpose). Vulnerabilities that cannot be detected in an automated manner (especially business logic vulnerabilities, vulnerabilities that need to be identified based on a comprehensive assessment of the environment, and others) are identified manually.

After the identification of vulnerabilities, it is verified whether these are not false-positive, and vulnerabilities are assessed in unity also in relation to other vulnerabilities.

When assessing vulnerabilities, exploitation of the vulnerabilities is not part of the process.

IstroSec offers these types of vulnerability assessment:

- External vulnerability assessment
- Internal vulnerability assessment
- Cloud vulnerability assessment
- vulnerability assessment of application or application endpoint

Vulnerability assessment should be performed according to the type of organization:

- Continuous (for organizations with high security requirements)
- Once per month (for organizations with increased security requirements)
- Once per 6 months (for organizations with standard security requirements)
- Once per year for other organizations

Vulnerability Assessment Program

For some organizations, due to their security requirements and security profile, it is appropriate to build their own vulnerability assessment program.

- The program consists of the following components:
- Infrastructure analysis and vulnerability assessment program design
- Implementation of technical prerequisites for the vulnerability assessment program:
  - test equipment (network and application vulnerability scanners)
  - automation of evaluation
- Design and implementation of vulnerability assessment processes
- Training of specialists to perform vulnerability assessment
- Design and implementation of program development processes

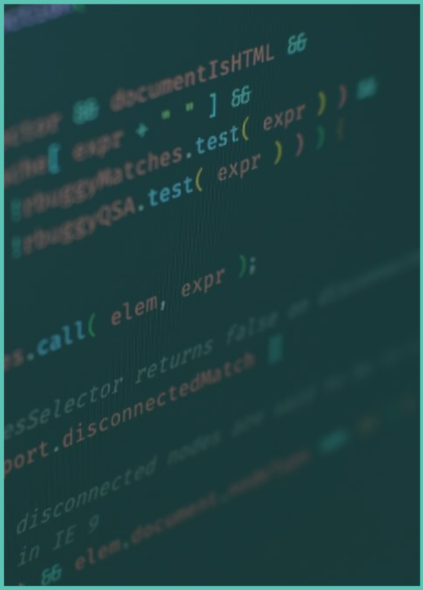
Why IstroSec?

Combined experience of more than 70 years

Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Certified experts to ensure compliance with security standards and legislation - **Istro**Sec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)



Case Study

Company type: manufacturing company
Service provided: vulnerability assessment
Solution:
The organization contacted us to find out what publicly available services and systems it has and then perform a vulnerability assessment on all identified IP addresses that belong to it. In the initial phase, we performed the Open-source intelligence (OSINT), during which we obtained a range of IP addresses belonging to the client company using a combination of different techniques. Additionally, we performed subdomain enumeration and domain identification. The techniques used included DNS brute-forcing, Certificate Transparency (CT) searches, browsing various websites such as github.com, pastebin.com, shodan.io, censys.io and others. The customer received a list of identified IP addresses and websites in a report from the enumeration part of the testing. After that, a test range was defined based on the data from this report. On this range, we performed automated port scanning, identified open ports, running services and their versions, SSL / TLS vulnerabilities and more. Subsequently, we manually verified each identified vulnerability, and we did not exploit these vulnerabilities. The result of the testing was a list of identified vulnerabilities and a way to eliminate them. Vulnerabilities were manually verified to prevent false-positive vulnerabilities, which saved the client time during the mitigation phase.

Penetration Testing

Penetration testing (ethical hacking) is the authorized intrusion into a customer’s networks, applications, or infrastructures to assess the level of security of these components from an attacker’s perspective. In contrast to vulnerability assessment, penetration tests include exploitation of identified vulnerabilities, post-exploitation (assessment and testing of the possibilities that an attacker can exploit on a system in tested network or infrastructure), lateral movement within the permitted scope and search for other vulnerabilities and re-exploitation.

IstroSec Offers These Types of Penetration Testing:

External penetration test:

- Web application and application endpoints
- Network penetration test
- Social engineering (phishing, spearphishing, smishing, vishing)

Internal penetration test:

- Application penetration test
- Network / infrastructure penetration test
- Penetration test of Active Directory

Platform-specific tests:

- Cloud penetration test
- Mobile application penetration test
- Wireless penetration test

Complete penetration testing includes both manual and automated testing to obtain sensitive data and penetrate as far as possible (within the pre-agreed scope of testing, of course). Also, the goal is to point out the attacker's possible ways to get access, the subsequent escalation of privileges to a higher level and the use of vulnerabilities found to compromise the system.

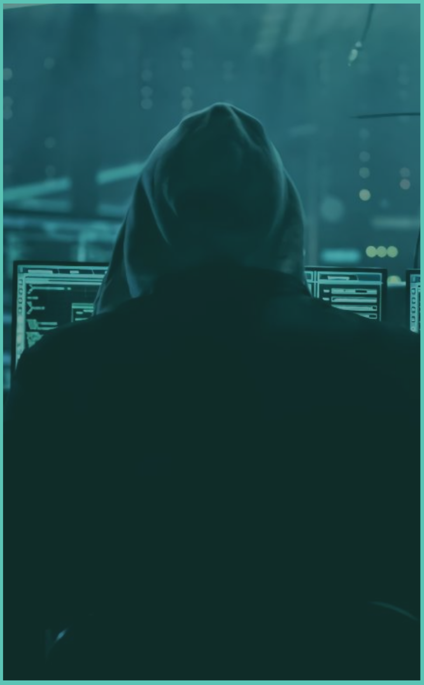
Testing takes place in several phases in order to detect and point out weak points, either from inside or outside the tested system.

After completing the last phase of penetration testing, the client will receive a final report which contains:

- executive summary
- the overal state of security of the tested system
- vulnerabilities found in detail and their risk level
- recommendations based on the identified environment
- recommentations to mitigate identified vulnerabilities

Who Is Penetration Testing For?

Especially for organizations that want to check the current state of the system or network from the security point of view and automated testing services such as vulnerability scanning, or vulnerability assessment is not enough for them. These types of organizations require thorough testing to detect as many weaknesses as possible and they want to know where and how far the real attacker could go. As penetration testing actively exploits the already identified vulnerabilities, it is possible to determine how could the attacker exploit these vulnerabilities to cause negative impact.



Case Study

Company type: digital marketing company
Service provided: web application penetration testing
Solution:
The client asked us to assess the security of a web application and its components. In this case, the web application penetration testing service was used, which includes testing using the OWASP Testing Guide v4.2 methodology together with our proven and functioning procedures. The penetration test was a black-box test, which means that we were not provided with data on how the application works. It was up to us to reveal the entire surface of the application which could be attacked from the external environment. The client was also interested in testing the REST API, where several critical vulnerabilities were identified. The result of the testing was the identification and correction of several errors in the test version of the application, which allowed its deployment in production only after the mitigation of security risks was performed. At the end of testing, the client received a final report. It contained an executive summary, a detailed description of the identified vulnerabilities, their mitigation strategies and a conclusion summarizing the security status of the tested application. If the client is interested in verifying that vulnerabilities have indeed been properly addressed, test results can be delivered on the fly during testing.

Red Teaming

Red team engagement uses tactics, techniques, and procedures (TTP) to simulate real cyber threats based on an organization's security profile. The entire red team, in addition to verifying the organization's cyber security level, helps the organization's defense team detect and respond to a cyber-attack.

The goal of the red team is also to simulate a realistic attack on the organization, which is based on relevant threats and TTPs for the organization. In this simulation, the goal is also to examine security measures, technologies, processes, the organization's security team and identify possible deficiencies.

Red teaming is usually performed without the knowledge of the organization's security team, except for a few selected employees.

Red Teaming Phases:

Creating a threat profile for the target organization and passively and actively obtaining information about the organization:

- Passive reconnaissance (including OSINT and DarkWeb Search)
- Active reconnaissance

Scheduling attacks to achieve set goals (such as accessing specific data, controlling infrastructure, compromising a specific user, running code on an organization's devices, and so on) and defined constraints.

Initial attack vectors usually include:

- attacks on the user (social engineering),
- attacks on user devices,
- perimeter attacks on the organization,
- attacks on remote assets of the organization (especially cloud services),
- (optional) physical security and
- (optional) supply chain attacks.

Execution and documentation of attacks (successful and unsuccessful) and implementation of steps to achieve the set goals. This step usually includes:

- escalation of privileges on the machines and information systems and other post-exploitation activities,
- distribution of tools and modified malicious code within the scope of specified targets,
- lateral movement between systems and other necessary steps depending on the goals specified by the organization.

Creating a report from the red teaming engagement, which includes:

- list of successful attack vectors,
- identified vulnerabilities in the target organization,
- proposed security controls and mitigations,
- timeline of activities performed and
- assessment of the effectiveness of the implemented security controls.

Case Study

Company type: financial institution
Service provided: red teaming
Solution:
A financial institution approached us with a request to simulate an attack using red teaming, which would verify the resilience of the entire external and internal infrastructure to cyber threats. This type of simulation has several advantages over a classical penetration test. It does not focus only on a narrowly defined test scope, such as a pair of web applications or possibly part of a network, but on everything that falls under the tested organization, and is agreed in advance within the test scope. Another indisputable advantage is the possibility of using social engineering. Therefore, if the organization has a small number of systems available from the Internet, if they do not lack patch management, and if it is not possible to to use these systems to penetrate the organization's internal network, red team will try to find another way in, for example, through spearphishing and a narrowly profiled campaign. The simulation of attacks used by attackers is performed by experienced ethical hackers with training and certifications in this area. In this case, red teaming helped the organization find vulnerabilities that even regular penetration tests and vulnerability assessments were not able to discover. We pointed out several points through which an attacker could penetrate the network. We used techniques that allowed us not to draw attention to ourselves and avoid detection by the blue team, whose task was to stop us. The defined goal at the beginning of the simulation was to obtain a domain administrator account, and to access the shared disk storage where the sensitive data was located. We were able to compromise the domain, using spear-phishing to gain initial access to the network. At the end of the simulation, the customer received a final report with an executive summary, a list of strengths and weaknesses, a detailed description of how we proceeded to compromise the domain, identified vulnerabilities with a description of how to remove them and other useful information. In the customer's organization, only a minimum number of employees knew about the red teaming exercise. To avoid disclosure, the blue team could not have any information about it.

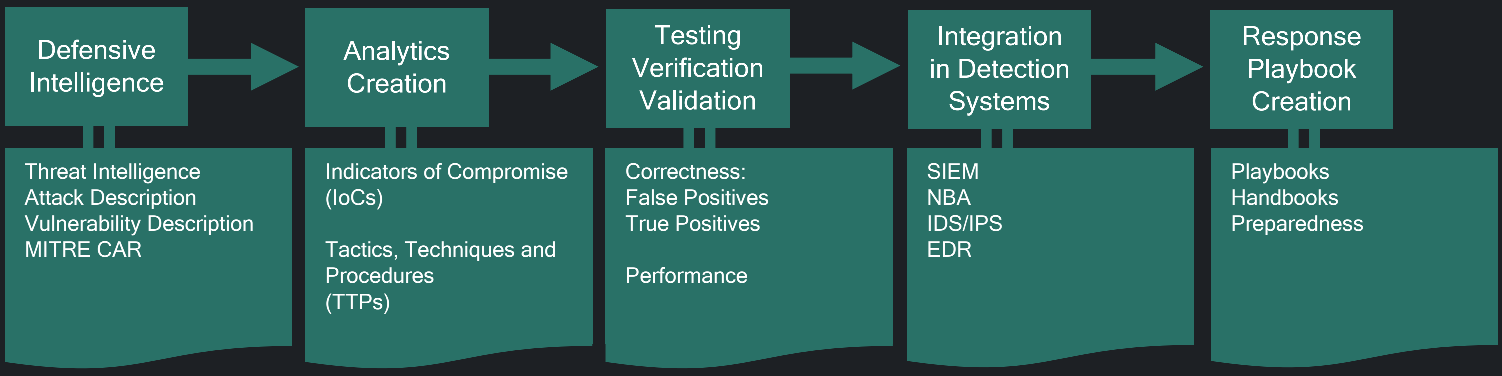
Purple Teaming

For organizations with increased security requirements, as well as for organizations that are long-term targets of advanced attackers, it is necessary to continuously implement security measures and detections for current security threats.

In purple team engagement, **Istro**Sec focuses on people, processes and technology.

Based on this approach, we:

- establish the necessary processes, guidelines, and procedures for purple teaming,
- train the internal security team,
- design and implement the necessary technologies,
- identify relevant resources and implement analytics based on this methodology.



Defensive Intelligence

Threat Intelligence
Attack Description
Vulnerability Description
MITRE CAR

Analytics Creation

Indicators of Compromise (IoCs)

Tactics, Techniques and Procedures (TTPs)

Testing Verification Validation

Correctness:
False Positives
True Positives

Performance

Integration in Detection Systems

SIEM
NBA
IDS/IPS
EDR

Response Playbook Creation

Playbooks
Handbooks
Preparedness