IstroSec

Data Sheet

Managed Defense

These days during the increased number of ransomware, phishing and other malicious activity, the need for systematic and continuous monitoring of your organizations IT infrastructure keeps increasing. Our cybersecurity monitoring services include activities that are usually performed using cyber security solutions capable of analysis and report generation.

The service includes:

- Network monitoring – IDS and IPS
- Endpoint process monitoring – EDRs
- Collection and log correlation – SIEM tools
- Automatization of investigative and reactive processes – SOAR tools

> *Delegating these activities to a specialized SOC team improves the focus and quality of the work and makes the monitoring operation more accessible.*

Service levels

- **L1** – Monitoring and and basic analysis of reports generated from monitoring tools
- **L2** – Advanced analysis of alerts within monitoring tools
- **L3** – In-depth analysis of suspicious activity directly on the affected device, acquisition and analysis of data from sources outside of monitoring tools

Possible verdicts on the analyzed activity

- **Malicious** - The activity has been confirmed to be malicious
- **Suspicious** - The activity can be interpreted as malicious or potentially undesirable under certain conditions. The context of the activity provided by the client is crucial.
- **Harmless** - The activity was corelated with the harmless activity and the monitoring tool report was a false positive

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 - IstroSec 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)

IstroSec

Data Sheet

Prerequisites

L1

- API keys enabling data collection from monitoring tools
- Access to the client's infrastructure security monitoring tools
- Escalation contacts on the client's side

L2

- Rights to execute queries, read and aggregate logs from devices
- Access to the client's infrastructure security monitoring tools
- Escalation contacts on the client's side

L3

- Administrator access to client endpoints, unless an EDR tool with equivalent functionality is deployed
- Escalation contacts on the client's side

Service Packages

Package 1

- 8/5 monitoring and analysis of alerts from monitoring tools on levels L1, L2 and L3
- Reporting the verdicts “Malicious” and “Suspicious” to the client
- Alerting the client in case of internal escalations to L3 regardless of reaching the final verdict

Package 2

- 8/5 emergency to receive L2 and higher escalations and their analysis
- Internal escalation to L3, if needed
- Feedback to the client regarding the verdict

Package 3

- 8/5 emergency to receive L3 and higher escalations and their analysis
- Feedback to the client regarding the verdict

All the packages contain:

- Regular reporting on the activity via monthly summary report

Optional for each package:

- Management of supported software tools for cybersecurity monitoring
- Ad-hoc configuration check of supported cybersecurity monitoring tools in place
- Assistance with the deployment of supported tools for cybersecurity monitoring
- Regular video call with an **Istro**Sec analyst reporting on monitored activity
- Ad-hoc video call with an **Istro**Sec analyst to discuss a report escalated from **Istro**Sec to the client

IstroSec

Data Sheet

Why Us?

Experience and knowledge

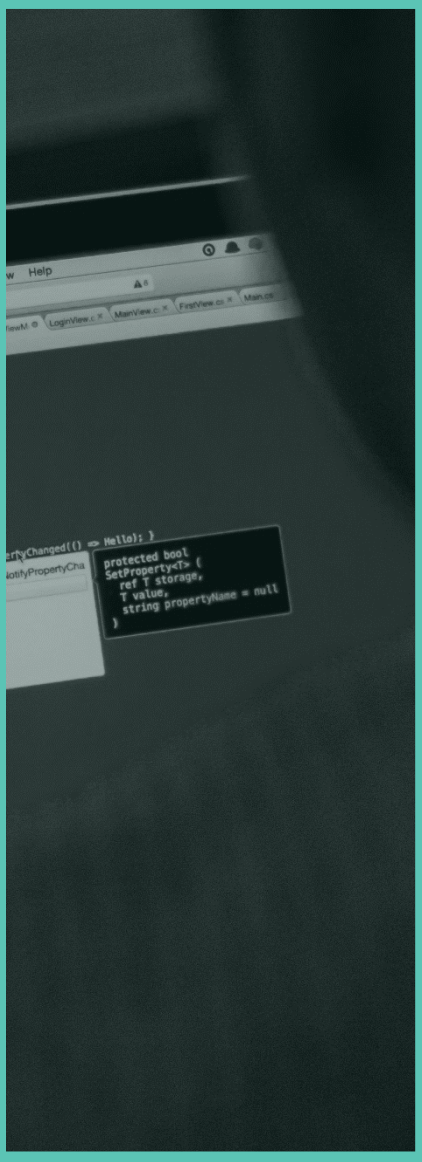
IstroSec specialists have experience in managed defense, security monitoring and security incident response according to current best practices using a variety of technologies. They know the tactics, techniques, and procedures of attackers and have the knowledge necessary to enable you to make decisions during incident response based on an analysis of the attackers' activities during in the attack.

Expertise in managed defense

Expertise in managed defense, incident response and many other areas of information security, such as information security management, audit, or world-class malware analysis, which we have repeatedly demonstrated while dealing with state-sponsored cyber-attacks, attacks on Fortune 500 organizations, as well as the participation of four **Istro**Sec experts in the winning team of Locked Shields 2016 exercise.

Certified professionals

IstroSec experts are also holders of internationally recognized certificates in these areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA), CCFA, CCFR, CCFH and more.



Case Study

Company type: Organization from the energy sector

Service provided: Managed defense

Solution: Managed defense of infrastructure on level L3, Package 1

The organization has an EDR solution deployed on all workstations and servers. The **Istro**Sec operator performing L1 monitoring responds to a message generated by the analytical functionality of the EDR solution with a description of an unusual command line execution on one of the servers. The message is escalated to the L2 level and the operator performs the following analytical steps:

- Analysis of the command executed by the cmd.exe process contains two consecutive commands, separated by &&. The first restarts the known and harmless system service, and the second creates a scheduled task with a trusted-looking name indicating a relation with the system service.
- The review of freely available documentation does not contain any mention of the existence or purpose of the scheduled task with this name. The preliminary verdict on the activity is internally as suspicious to malicous.
- EDR is used to analyze the hierarchy of processes that led to the execution of the suspicious command. One of the processes has its executable file located in the AppData\Roaming folder, which is where the malware often hides. The alert is escalated to the L3 level and the preparation of the report for the client is started.
- Within the EDR functionality, queries are made to the identify the timeframe of the activity:
  - Determining the time when the suspicious file hash was first seen on the device that generated the alert.
  - List of all devices on which the hash was detected, date and time. Hash has also been seen a few hours earlier on a server that is accessible from the Internet to provide the organization's services to its customers. The location of the file is consistent with exploitation of the vulnerability in the web application.
- A security incident is declared, the client is sent a report with current findings and recommendations on how to proceed during incident response. The **Istro**Sec monitoring team supports the response and investigation using EDR to look for additional evidence when containing the incident and acquires evidence and logs for detailed analysis.
- Using the EDR and with the consent of the client, a sample of a given suspicious file is acquired to perform a malware analysis.
- Directly from the affected devices, the operator identifies the MACB values of the timestamps of the file as well as the configuration file of the suspicious scheduled task.
- All indicators of compromise (IoCs) found using EDR, malware analysis, and forensic analysis are marked within the EDR to generate reports when they are detected.

IstroSec | Černyševského 10 | 851 01 Bratislava | Slovakia | +421 917 699 002 | info@istrosec.com | www.istrosec.com