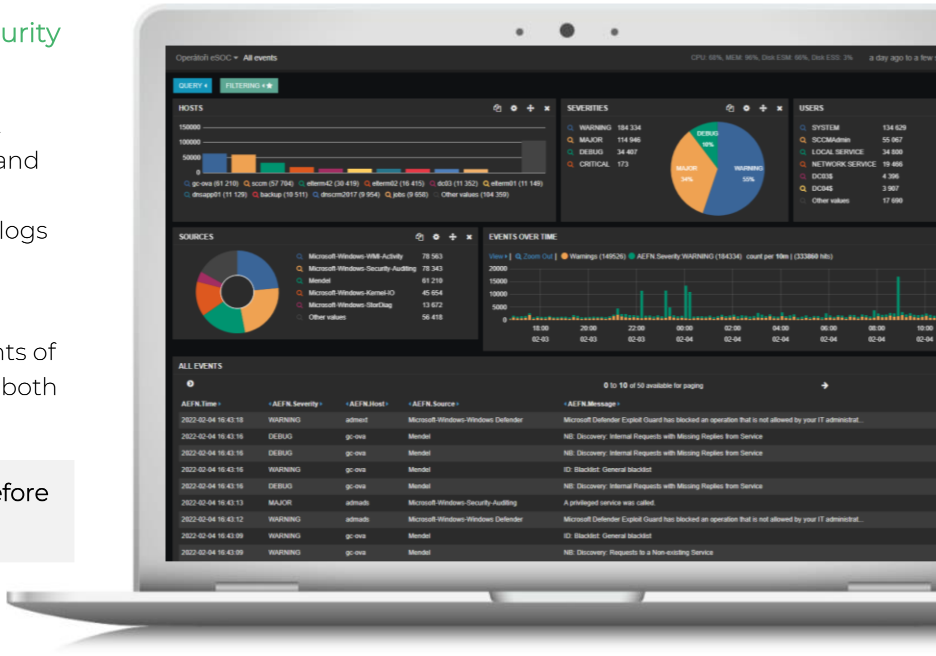
LOG MANAGEMENT / SIEM
ELISA SECURITY MANAGER

How to easily collect and evaluate cybersecurity and operational events?

ELISA Security Manager is a robust, powerful, yet cost-effective solution for collecting, correlating and log analysis. The system provides a high level of convenience for analysis of detected events and logs with click-through to visual rule editor.

The solution will meet the needs of most organizations and complies with the requirements of the Cyber Security Act security requirements for both major and critical information systems.

Detect and fix infrastructure problems earlier, before they negatively impact your organization.



AEFN.Time	AEFN.Severity	AEFN.Host	AEFN.Source	AEFN.Message
2022-02-04 16:43:18	WARNING	admext	Microsoft-Windows-Windows Defender	Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT administrat...
2022-02-04 16:43:16	DEBUG	gc-ova	Mendel	NB: Discovery: Internal Requests with Missing Replies from Service
2022-02-04 16:43:16	DEBUG	gc-ova	Mendel	NB: Discovery: Internal Requests with Missing Replies from Service
2022-02-04 16:43:16	WARNING	gc-ova	Mendel	ID: Blacklist: General blacklist
2022-02-04 16:43:16	DEBUG	gc-ova	Mendel	NB: Discovery: Internal Requests with Missing Replies from Service
2022-02-04 16:43:13	MAJOR	admads	Microsoft-Windows-Security-Auditing	A privileged service was called.
2022-02-04 16:43:12	WARNING	admads	Microsoft-Windows-Windows Defender	Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT administrat...
2022-02-04 16:43:09	WARNING	gc-ova	Mendel	ID: Blacklist: General blacklist
2022-02-04 16:43:09	WARNING	gc-ova	Mendel	NB: Discovery: Requests to a Non-existing Service

WHAT ELISA CAN HELP YOU WITH

As infrastructure grows, it is difficult to have a comprehensive overview without a dedicated tool. The solution is to have one system dedicated to directing all events and information.

Do you often deal with questions like: who deleted files on a shared drive? Who made a change to the database? Who is trying to guess the access password?

Are you looking for a cybersecurity event collection and assessment tool that adapts to your needs and is standards compliant?

Do you run your own monitoring center and need a central console to handle events by operators of the monitoring center?

Do you use multiple security systems and would like to consolidate information into one platform?

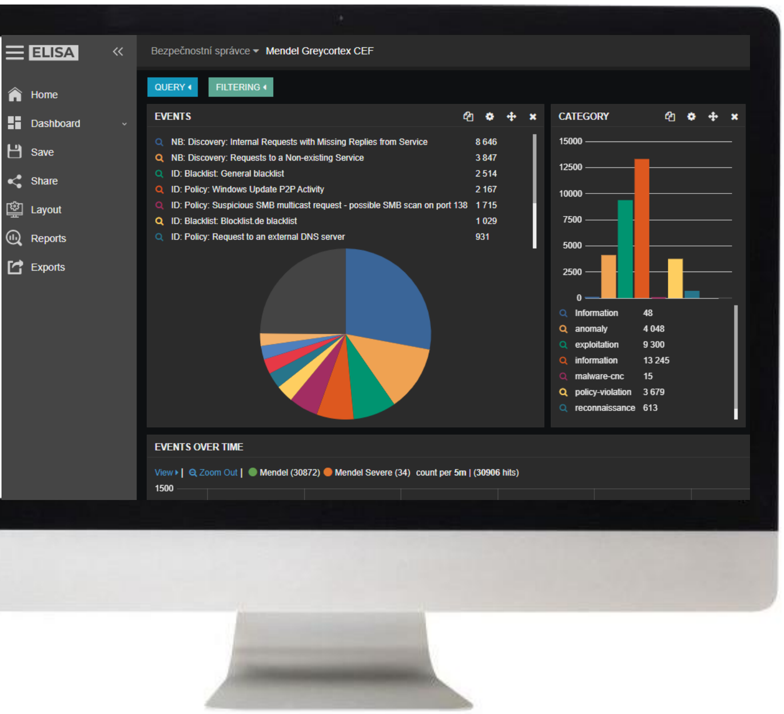
ONE SOLUTION, MANY ADVANTAGES

- Central security monitoring console.
- Visibility and quick problem analysis.
- Comprehensive tool for SOC operations.
- Compliance with laws and standards.
- Interactive interface, including visual rule editor.
- Support for contextual correlations.
- Integration with OpenVAS, GSM, Flowmon, Greycortex
- Integration with Microsoft Cloud (Azure, Office 365)
- Built-in „Change auditor“.
- Central agent management.
- Distributed log collection.
- Calculation of risk level for each event.

WHAT MAKES US DIFFERENT

- Integrated ZABBIX operational monitoring.
- Scalability and customization of implementation.
- Integrated ticketing system.
- Support for all text-based logs.
- Solution coordination and proactivity of our specialists.
- Czech manufacturer with direct technical support.
- Interface and documentation in Czech language.
- Low acquisition costs.
- High performance (up to 10 000 EPS).

> *ELISA at one of our customers achieved improved results within 3 months when evaluating and event investigation than their previous SIEM over 3 years. Plus, at a fraction of the cost.*



EVENTS	
NB: Discovery: Internal Requests with Missing Replies from Service	8 646
NB: Discovery: Requests to a Non-existing Service	3 847
ID: Blacklist: General blacklist	2 514
ID: Policy: Windows Update P2P Activity	2 167
ID: Policy: Suspicious SMB multicast request - possible SMB scan on port 138	1 715
ID: Blacklist: Blocklist.de blacklist	1 029
ID: Policy: Request to an external DNS server	931

CATEGORY	
Information	48
anomaly	4 048
exploitation	9 300
information	13 245
malware-cnc	15
policy-violation	3 679
reconnaissance	613

Mendel (30872) Mendel Severe (34) count per 5m | (30906 hits)

FROM LOG MANAGEMENT TO SIEM

Advanced correlations

ELISA includes an advanced correlation mechanism with support for contextual correlations over time intervals of up to several months. It can easily detect security incidents - for example, based on recurring elementary events, but also the spread of hidden malware on the network or users logging into an application after several weeks of inactivity.

Calculating the risk score

The system allows events to be enriched with data from external sources and calculates a so-called "risk score" for events, which makes it easy to prioritise the steps leading to the resolution of indicated alarms. It also supports integration of Cyber Thread Intelligence sources according to STIX/TAXII standard or white and blacklists in any format.

Change detection of configurations

The solution also includes support for periodic configuration auditing (Change Auditor). ELISA includes a File Integrity Monitoring and Registry Integrity Monitoring module.

Event and Incident Investigation

Another advantage is the clear internal ticketing, which builds on the MITRE ATT&CK® and MISP taxonomy. It provides a visualization of the time progression of each phase of an incident or attack

Integration and supported devices

With support for standard protocols and industry standards, ELISA supports the integration of virtually any tool at the security alarm processing level, including cloud applications such as Microsoft Cloud App Security (Azure, Office 365) or trace log collection from Exchange Onlinez Exchange Online.

OFFERED EDITIONS

	SIEM	LM
Log collection and processing	✓	✓
Visual rule editor	✓	✓
Pre-built dashboard sets	✓	✓
Integrated operational monitoring	✓	✓
Integration with third-party systems	✓	✓
Advanced contextual correlations	✓	
Correlation with existing vulnerabilities	✓	
Change detection of configurations	✓	
Enrichment of events from other sources	✓	
Internal ticketing	✓	
Calculating risk scores	✓	

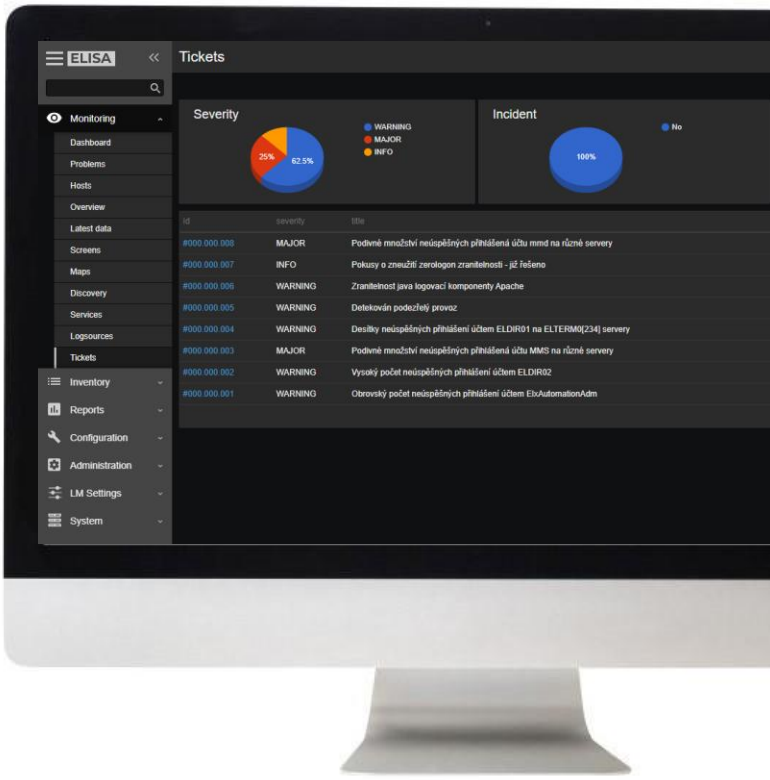
DEPLOYMENT MODELS

Physical Appliances are a complete solution in the form of a pre-installed physical server that are optimized to process up to 10,000 events per second (EPS) on a continuous basis and receive up to 30,000 EPS on a short-term basis.
The system throughput and central log storage capacity can be increased by horizontal scaling, i.e. by acquiring additional devices and performing a clustered installation. ELISA is also available as a virtual appliance (VMware, Hyper-V). With sufficient allocation of performance resources, analogous throughputs can be achieved in a virtual environment. The performance of a distributed data acquisition system can also be increased by vertical scaling.

LICENSING

The software license (annual subscription) is licensed according to the number of monitored devices. The basic license starts at 50 devices up to an unlimited license.

We will be happy to help you choose the right edition.



id	severity	title
#000.000.008	MAJOR	Podivné množství neúspěšných přihlášená účtu mmd na různé servery
#000.000.007	INFO	Pokusy o zneužití zerologon zranitelnosti - již řešeno
#000.000.006	WARNING	Zranitelnost java logovací komponenty Apache
#000.000.005	WARNING	Detekován podezřelý provoz
#000.000.004	WARNING	Desítky neúspěšných přihlášení účtem ELDIR01 na ELTERM0[234] servery
#000.000.003	MAJOR	Podivné množství neúspěšných přihlášená účtu MMS na různé servery
#000.000.002	WARNING	Vysoký počet neúspěšných přihlášení účtem ELDIR02
#000.000.001	WARNING	Obrovský počet neúspěšných přihlášení účtem ElxAutomationAdm