ELISA

Security Manager

novicom

Tool for intercepting and evaluating cybernetic security events

The Novicom ELISA Security Manager is a robust, powerful yet **highly cost-effective solution for collecting, correlating and analysing logs.** The system provides a high level of convenience for the analysis of detected security incidents and the relevant logs.

The user interface is a web browser. Searching through the database is similar to using an internet search engine. After a short training session, even an inexperienced user will be able to prepare complex filters. The ELISA tool was originally developed as a **log management system which has been gradually enhanced to a more complex SIEM-type tool.**

Novicom ELISA Security Manager also utilises an advanced correlation engine supporting contextual correlation, even over periods of several months. This allows the **detection of cybersecurity events**, not only through repeated elementary incidents, but also the spread of hidden malware over a network or users signing into applications after several weeks of inactivity.

The **ELISA allows you to enrich the events with information from external sources** and calculates a "risk score" for all events, allowing one to easily prioritise the steps needed to resolve alarms that appear. The ELISA includes support for regular monitoring of configurations (the so-called Change Auditor) and other advanced SIEM functions.

What information can the ELISA solution uncover?

Overview of functional features

ELISA

APPLICATION OR SYSTEM ERRORS ALERT

- **SOPHISTICATED CORRELATION EVALUATION**
  - Security incident detection
  - Suppression of false alarms and notifications
- **SPECIFIC INDIVIDUAL ERRORS**
  - More flexible than conventional performance monitoring (Nagios, Zabbix,...)
- **INTELLIGIBILITY**
  - Translation of error codes
  - Translation of IP addresses to DNS names

SECURITY MONITORING

- **CENTRAL ALARM CONSOLE**
  - Antivirus system
  - Intrusion Prevention System (IPS)
  - Data Loss Prevention System (DLP)
- **IMPACT ANALYSIS**
  - To whom was an infected e-mail attachment delivered?
  - Which stations are showing symptoms of virus infection?
  - Which user accounts were compromised during the attack?

PERFORMANCE MONITORING

- **INTEGRATED ZABBIX SYSTEM**
  - Graphical representation of availability and network traffic
  - Fully automated monitoring of VMware infrastructure
  - End-user monitoring of web applications
  - Evaluation of SLA fulfillment by the supplier

ANALYSIS OF NETWORK TRAFFIC

- **WEB PROXY**
  - Most visited sites
  - Largest data downloaders
- **WEB SERVER**
  - From which cities do people access the system?
  - Detection of broken links on the company website
- **FIREWALL, ROUTER**
  - Detection of port scanning by an attacker
  - Detection of DoS and DDoS attacks
- **INTERNAL SWITCH**
  - Which applications have the greatest burden on the network?
  - Which devices generate the most network traffic?
  - Control access control device to the network 802.1x

AUDITING OF CHANGES AND ACTIVITIES

- **DATABASE**
  - Who changed the bank account number?
  - Who has viewed employees' personal information?
- **DOCUMENTS AND FILE SYSTEMS**
  - Who deleted the tender documents?
  - Who copied an unusual number of drawings?
- **CONFIGURATION CHANGES**
  - Network elements and security devices
  - Directory services and operating systems
  - Applications and databases
- **COMPLIANCE WITH STANDARDS**
  - ISO 27001
  - Cyber Security Act
  - PCI, SOX and more

Key properties

- Automatic evaluation
- Security risk detection
- A clear and simple web user interface
- Compliance with the Cybersecurity Act, GDPR, ISO, PCI
- Built-in Change Auditor
- Further advanced SIEM functions
- Integration with tools for network monitoring and management
- Physical and virtual appliances
- Distributed log collection
- Horizontal scalability
- High performance (up to 10 000 EPS)
- Low initial costs
- Designed for embracing of advantages of strategy of active SOC advantages

ELISA – technologies used

Thanks to its architecture ELASTICSEARCH provides lightning-fast responses even with large indexes/databases. The basic user view shows a histogram with the number of matching events in a selected time interval and a paged table summary.

When configured properly, the ELISA solution records events in the analytic database in their original form and structure, with seamless support for diacritics.

By selecting a specific event, users can open an overview of all its attributes and perform drilldown analyses.

Selecting any attribute returns a statistical overview of the distribution of its values, enabling quick filtering (including negative) by any given value.

NXLOG is an agent **designed for installation on monitored systems** that cannot process and send log records autonomously. NXlog supports the interception of events from text logs, Windows event logs, various types of structured logs (CSV, j2log and many more) and relational database tables.

PRIMARY FEATURES OF NXLOG:

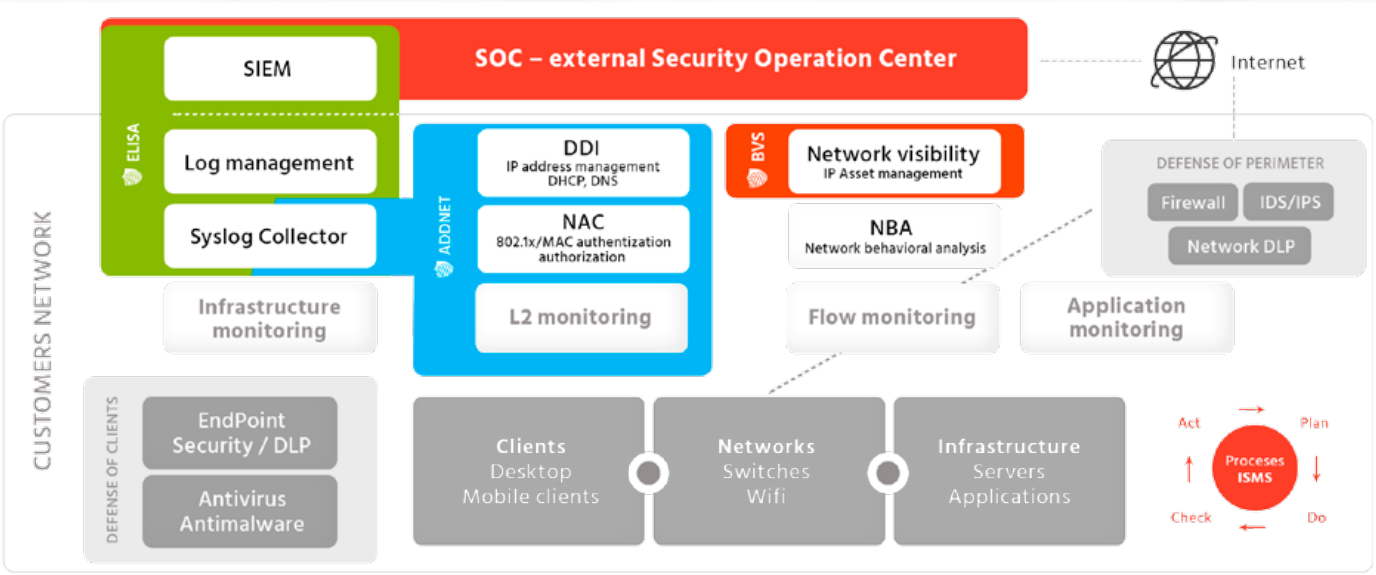
- Multiplatform agent that is easy on resources
- Creates a buffer of events if the central system is unavailable.
- Remembers the position of processed events even after a restart.
- Supports rotated log files, various encoding types and multi-line records.
- Enables filtering and correlation of events in the monitored system.
- Supports the transfer of structured records in a binary format and over encrypted connections (TLS).

Specifications of the Novicom ELISA models on offer

Physical appliances are a **complete Novicom ELISA Security Manager system** in the form of a pre-installed physical server with "On-Site Service" hardware "the next business day" for 5 years.

Model	Throughput (EPS)	Capacity storage	Retention estimate (half EPS)	Storage resistance (RAID)	Redundant power supply
ESM Appliance XL	10 000	100 TB	12 Months	2 Disks	Yes
ESM Appliance L	6 000	42 TB	9 Months	2 Disks	Yes
ESM Appliance M	2 000	12 TB	8 Months	1 Disk	Yes
ESM Appliance S	1 000	4 TB	3 Months	1 Disk	Yes

The throughput of the ELISA Security Manager system and capacity of the central log storage may be increased by horizontal scaling, i.e. the purchasing of further devices and implementation of a cluster setup. **Novicom ELISA Security Manager is also available as a virtual appliance** (VMware, Hyper-V). With allocation of sufficient power resources, analogous throughputs may be achieved even in a virtual environment. **The performance of the distributed data collection system may also be enhanced using vertical scaling.**



ELISA and Active SOC

ELISA is an important part of the Active SOC (Security Operation Center) strategy, which Novicom, together with its SOC partners, is trying to promote on the market. **ELISA, together with the ADDNET solution** (for efficient management of network services and network access control) **and the BVS solution** (for visualization of network assets, including their connection to business services) **form a unique portfolio that prepares customers for fast and seamless connection to the SOC service**. Customers using this product platform can then take full advantage of Active SOC's premium services.

The Novicom ELISA is appreciated not only by security administrators, but also by administrators responsible for systems operation.

Thanks to this, selected SOC operators are able to guarantee a fully qualified active response to cyber attacks in the 24x7 mode without the necessary cooperation with the system administrators at the customer. This is fully in line with the current trend of using top security surveillance (SOC) as a service. **This approach eliminates the economic disadvantage** of acquiring a complete range of single-purpose technologies and the need to have an in-house highly specialized team able to face professional hackers at any time.

novicom

Novicom, s.r.o.
Prague, Czech republic

www.novicom.eu
sales@novicom.eu

ELISA