

eurofunk SIEM

Security Information and Event Management

NIS2-konforme Sicherheit für Leitstellenbetrieb

PRODUCT | SOLUTIONS | SERVICE

 **eurofunk**
creating safety by technology

Über uns

eurofunk Innovation und Sicherheit vereint

eurofunk ist einer der führenden Systemspezialisten für die Planung, Errichtung und den Betrieb von Leitstellen und Notrufzentralen. Mit einem umfassenden Produktportfolio und einer einzigartigen Lösungskompetenz bieten wir 360°-Lösungen und -Services für Organisationen der öffentlichen Sicherheit, Industrie und Flughäfen. Profitieren Sie von unserem ganzheitlichen Ansatz und unserem jahrzehntelang gewachsenem Know-how im Bereich der Leitstellentechnologie. Wir bieten Ihnen modernste Lösungen, die auf Ihr Unternehmen maßgeschneidert sind und Ihren individuellen Ansprüchen entsprechen.

Von der ersten Planung bis zur finalen Umsetzung und darüber hinaus – eurofunk Kappacher steht für Qualität, Zuverlässigkeit und Innovation.

Key Facts

Familiengeführtes Unternehmen seit 1969

Über 30 Jahre spezialisiert
auf Leitstellentechnologie

Vier Jahrzehnte Know-how in
Analog- und Digitalfunk

Beschäftigt mehr als 600 Mitarbeiter

eurofunk.
creating safety by technology



Command & Control
Solutions (CAD)



Multimedia
Solutions



IT Solutions



Communications
Solutions



Control Room
Design



360° Service

“ Im Herzen des
Salzburger Landes





eurofunk SIEM

Zentrale Sicherheit für eine verfügbare und NIS2-konforme Leitstelle

In Integrierten Leitstellen steht die Verfügbarkeit der Systeme an oberster Stelle. Gleichzeitig nehmen Cyberangriffe kontinuierlich zu und mit der NIS2-Richtlinie steigen die gesetzlichen Anforderungen an die IT-Sicherheit deutlich. Betreiber kritischer Infrastrukturen sind gefordert, Sicherheitsvorfälle frühzeitig zu erkennen, nachvollziehbar zu dokumentieren und angemessen darauf zu reagieren.

Sicherheitsanalyse mit klarem Nutzen

Die eurofunk SIEM-Lösung unterstützt ein strukturiertes und proaktives Sicherheitsmanagement. Als zentrales System sammelt sie sicherheitsrelevante Ereignisse aus der gesamten IT- und Systemlandschaft, wertet diese in Echtzeit aus und stellt Zusammenhänge übersichtlich dar. So können Auffälligkeiten und potenzielle Bedrohungen frühzeitig erkannt werden, bevor sie die Verfügbarkeit der Leitstelle beeinträchtigen.

Die Lösung wurde speziell für den Einsatz in kritischen Infrastrukturen und Leitstellenumgebungen entwickelt und berücksichtigt neben technischen Anforderungen auch die besonderen betrieblichen Rahmenbedingungen der Leitstellen.

Alle relevanten Protokolldaten werden zentral erfasst und revisionssicher archiviert. So entsteht eine nachvollziehbare Transparenz über sicherheitsrelevante Ereignisse und die Einhaltung zentraler Anforderungen der NIS2-Richtlinie, insbesondere in den Bereichen Detektion und Protokollierung.

Optional kann eurofunk SIEM in das eurofunk Aktive Monitoring (eAM) integriert werden. Dadurch wird auch der Systemzustand des SIEM zentral überwacht und in bestehende Überwachungsprozesse eingebunden.

Einblick in ausgewählte Features

The dashboard provides a comprehensive overview of system health and performance. It includes several key sections:

- System Information:** Displays core system details such as Version (5.0), Build (5016), Uptime (14 days, 20 hours, 26 minutes), System Time (28 Jan 2026 10:09:48), Hostname, Host IP, Current User IP, User (admin), and Last Login (2026-01-28 10:07:27).
- Summary Services:** A table listing various services and their status:

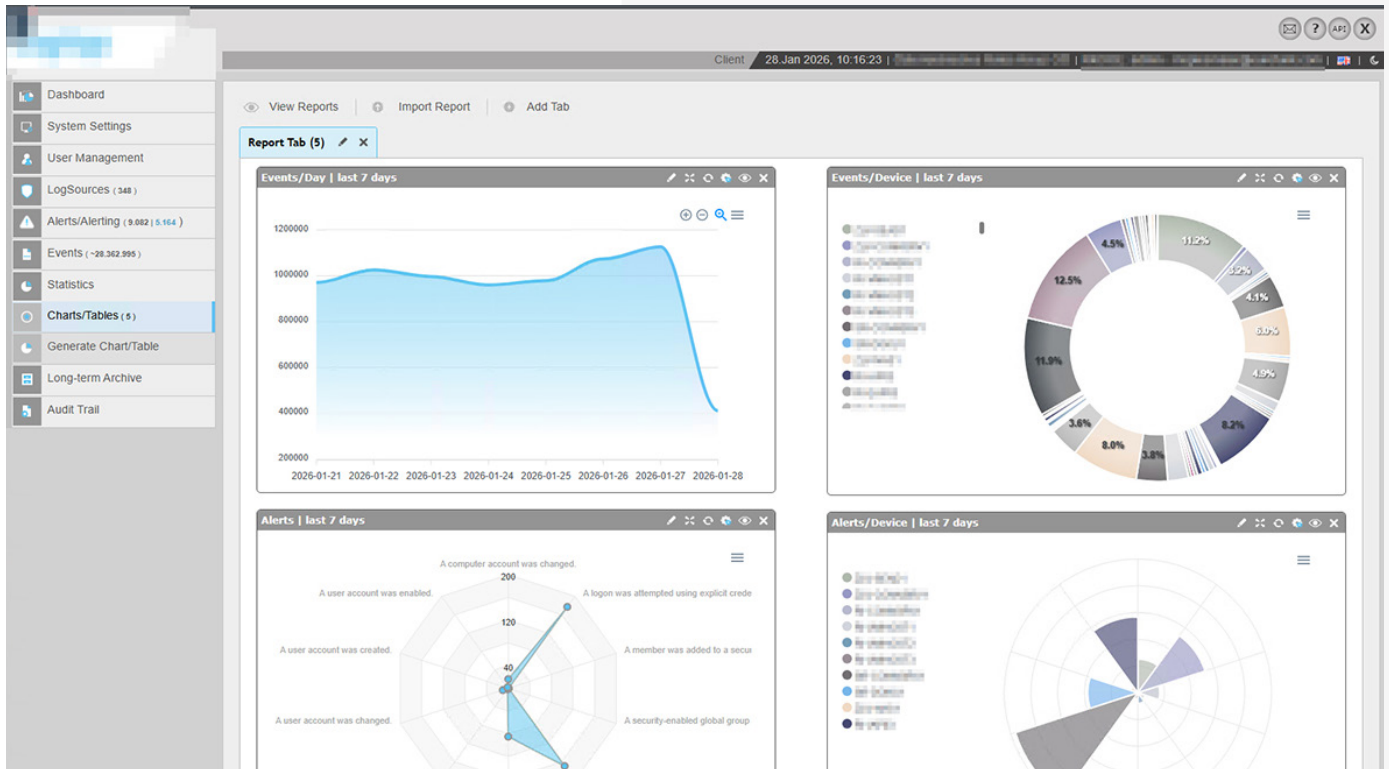
Name	Status
Heartbeat	🟢
Receiver	🟢
AlertParser	🟢
File Integrity	🟢
Reporting Engine	🟢
Indexer	🟢
LocalNetworkProxy	🟢
- Hardware Information:** Visualizes resource usage with progress bars: CPU (4%), Memory (65% of 31848 MB), HDD System (65% of 11 GB), HDD DB (16% of 3467 GB), and HDD Archive Share (6% of 50 GB).
- Log Statistics:** Shows overall activity counts: Server (~28,354,125), Network (~415,140), Vulnerability (0), Alerts/Alerting (9,082), and Alerts (9,082).
- User Authentication Log:** A detailed log of login and logout events, including timestamps and user identities.

Dashboard

The Alerts interface displays a list of system events, allowing for detailed investigation of each alert. The table below shows a sample of the data:

ID	Date/Time	Alert Name	Alert Message	Status	Device	Details
79823	2026-01-28 10:06:15	[Windows Security] Logon/Logoff	A service account was succe...	New
79822	2026-01-28 10:06:15	[WES] 16 > RDP Login	[WES] Remote Desktop login ...	New
79821	2026-01-28 09:50:34	[Windows Security] Account Management	A computer account was chan...	New
79820	2026-01-28 09:46:22	[Linux Security] Logon/Logoff	A user was logged off.	New	multiple	...
79819	2026-01-28 09:45:27	[WES] 02 > Application Crashes	[WES] Windows error reporting	New	multiple	...
79818	2026-01-28 09:36:35	[WES] 05 > Windows Firewall	[WES] Windows firewall rule...	New	multiple	...
79817	2026-01-28 09:36:00	[Linux Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79816	2026-01-28 09:36:00	[Linux Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79815	2026-01-28 09:36:00	[Windows Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79814	2026-01-28 09:21:13	[Windows Security] Account Management	A security-enabled local gr...	New	multiple	...
79813	2026-01-28 09:20:47	[WES] 15 > Pass the Hash	[WES] Pass the Hash Login A...	New	multiple	...
79812	2026-01-28 09:17:53	[WES] 11 > Defender	[WES] Defender: Protecting ...	New	multiple	...
79811	2026-01-28 09:16:45	[WES] 15 > Pass the Hash	[WES] Possible Pass the Has...	New	multiple	...
79810	2026-01-28 09:16:32	[Windows Security] Logon/Logoff	A logon was attempted using ...	New	multiple	...
79809	2026-01-28 09:14:27	[WES] 02 > Application Crashes	[WES] Windows application e...	New	multiple	...
79808	2026-01-28 09:12:06	[WES] 18 > Persistence	[WES] New scheduled task cr...	New	multiple	...
79807	2026-01-28 08:59:30	[Windows Security] Logon/Logoff	A service account was succe...	New	multiple	...
79806	2026-01-28 08:59:30	[WES] 16 > RDP Login	[WES] Remote Desktop login ...	New	multiple	...
79805	2026-01-28 08:57:59	[WES] 05 > Windows Firewall	[WES] Windows firewall rule...	New	multiple	...
79804	2026-01-28 08:57:51	[WES] 05 > Windows Firewall	[WES] Windows firewall rule...	New	multiple	...
79803	2026-01-28 08:56:14	[WES] 02 > Application Crashes	[WES] Windows application hang	New	multiple	...
79802	2026-01-28 08:50:20	[WES] 07 > Software and Service Installation	[WES] Windows: new MSI file...	New	multiple	...
79801	2026-01-28 08:45:40	[Linux Security] Logon/Logoff	A user was logged off.	New	multiple	...
79800	2026-01-28 08:45:25	[WES] 02 > Application Crashes	[WES] Windows error reporting	New	multiple	...
79799	2026-01-28 08:27:30	[WES] 10 > Group Policy Errors	[WES] Windows group policy ...	New	multiple	...
79798	2026-01-28 08:21:01	[Linux Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79797	2026-01-28 08:21:00	[Linux Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79796	2026-01-28 08:21:00	[Windows Self-Monitoring] Missing Statusreport	Statusreport is missing	New	multiple	...
79795	2026-01-28 08:20:46	[WES] 15 > Pass the Hash	[WES] Pass the Hash Login A...	New	multiple	...
79794	2026-01-28 08:16:37	[WES] 15 > Pass the Hash	[WES] Possible Pass the Has...	New	multiple	...
79793	2026-01-28 08:16:10	[Windows Security] Logon/Logoff	A logon was attempted using ...	New	multiple	...
79792	2026-01-28 08:12:54	[Windows Security] Account Management	A computer account was chan...	New	multiple	...
79791	2026-01-28 08:12:38	[Windows Security] Account Management	A security-enabled local gr...	New	multiple	...
79790	2026-01-28 08:09:25	[WES] 02 > Application Crashes	[WES] Windows application e...	New	multiple	...

Alerts



Report

Klare Verantwortung zwischen Betreiber und Systemanbieter

euromfunk SIEM ist als unterstützendes Werkzeug für die Systemtechnik konzipiert. Die Bewertung von Sicherheitsvorfällen, die Auswertung von Alarmierungen sowie die Einleitung geeigneter Maßnahmen liegen beim Betreiber. euromfunk stellt die technische Lösung bereit, die Verantwortung für die Sicherheitsstrategie bleibt klar geregelt.

euromfunk SIEM – eine verlässliche Grundlage für strukturierte IT-Sicherheit in Leitstellen.

SIEM



Website

www.eurofunk.com

Headquarters

eurofunk Kappacher GmbH
eurofunk-Straße 1 – 8
5600 St. Johann im Pongau
Österreich/Austria

Phone

T +43 57 112 - 0

T +49 7231 7782 - 0

