

Security Policy   
Event Handling

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Event Handling | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of Content

[1 Principle 4](#_Toc107986230)

[2 Objective 4](#_Toc107986231)

[3 Controls 4](#_Toc107986232)

# Principle

Security-related event logs must be regularly reviewed and analyzed using a combination of automated and manual methods.

# Objective

Detection of known vulnerabilities, unusual or suspicious activity and timely response to events that need to be investigated.

# Controls

An ITIL-based security incident management process must be established to identify, investigate and respond to security incidents.

The process of managing security events should be supported by:

* Security experts who are trained and experienced in dealing with security incidents (e.g. cyber security analysts, threat analysts or members of a SOC team)
* Products for managing security events (e.g. scanning software, log management tools and SIEM products)
* documented processes (e.g. for the analysis of cyber security events and the management of information security incidents).

The management of security information and events must be configured in such a way that:

* expected events can be identified (to reduce review and investigation activities for legitimate business events)
* unexpected events can be detected (to reduce the likelihood of false-positive and false-negative results)
* Anomalies in user behavior can be identified
* anomalies in IT system behavior can be identified
* confusing or misleading data (often referred to as "noise") generated by event logs can be analyzed.

The security event management process must include the capture of security events from all relevant logs, including:

* Application protocols
* System logs
* Protocols of network devices
* technical protocols (such as those of servers that support DNS, DHCP, FTP and SQL)
* Protocols of security products (e.g. malware protection software, data leakage prevention (DLP) and network intrusion detection (NIDS)).

The process for managing security events must cover the processing of important security-relevant events (e.g. through techniques such as normalization, aggregation and correlation).

The security event management process must cover the analysis and interpretation of security events by qualified analysts to detect unusual activity or anomalous behavior that may indicate a threat.

The management of security incidents must be supported by specific monitoring activities to identify and analyze anomalous behavior, e.g:

* Detect unauthorized scanning of business applications, information systems and networks
* Checking successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file shares)
* Check DNS logs to identify outbound network connections to malicious servers, such as those connected to botnet command and control servers
* Checking usage reports from service providers (e.g. invoices or service reports) for unusual activity in systems and networks (e.g. by checking activity patterns).

Suspected and actual information security incidents must be identified (e.g. infection with malware or abnormal communication behavior of IT systems) and be subject to further investigation (as part of the information security incident management and handling process).

Confirmed relevant information security incidents (such as cyber attacks) must be investigated by appropriately qualified persons.

Information on security incidents must be kept for at least 3 years.

In addition to processing internal security incidents in the corporate area, information on the general threat situation must be collected through contacts with special interest groups, analyzed and evaluated by SÜDVERS' technical experts and distributed promptly to the responsible operational units within SÜDVERS.