SAFELY ENABLING BUSINESS

Datasheet

# Standard Use Cases

## Use Cases im Einsatz bei SecureDetect SIEM – Security Analysis

*Der Service SecureDetect SIEM – Security Analysis basiert auf der Analyse von sicherheitsrelevanten Logdaten aus der IT-Infrastruktur unserer Kunden. Diese Logdaten werden durch ein SIEM-System gesammelt, das in diese Infrastruktur integriert wird.*

*Unsere Standard Use Cases decken verbreitete Angriffsszenarien ab. Sie erfüllen damit die Anforderungen aus verschieden Security Standards und Frameworks wie CIS Critical Security Controls, ISO/IEC 27001 oder PCI-DSS.*

| Name | Description | CIS Critical Security Control | ISO 27002:2014 | PCI-DSS v.3.2 |
|---|---|---|---|---|
| Usage of High Privilege Default Accounts | This use case looks for usage of default device accounts and a customer defined list of accounts that should not log in to the AD. | CSC 12: Boundary Defence | 9.2.2 User access provisioning | 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. |
| | | CSC 5: Controlled Use of Administrative Privileges | 9.2.3 Management of privileged access rights | 10.2.2 All actions taken by any individual with root or administrative privileges. |
| | | CSC 16: Account Monitoring and Control | 9.4.4 Use of privileged utility programs | |
| Malicious Outbound Connections | With the use of threat intelligence the SecureLink CDC monitor domains, IPs and other indicators of compromise that are engaged in malicious behavior. | CSC 8: Malware Defences | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| User Added to Critical Security Group | The CDC monitors user additions to groups such as domain admins and groups that the customer has chosen | CSC 5: Controlled Use of Administrative Privileges | 9.2.2 User access provisioning | 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. |
| | | CSC 16: Account Monitoring and Control | 9.2.3 Management of privileged access rights | 10.2.2 All actions taken by any individual with root or administrative privileges. |
| | | | | 10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. |
| Malware outbreak | This use-case is used to detect ongoing malware outbreak(s), where the same malicious code infects several machines within a very short timeframe. | CSC 8: Malware Defences | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| Ransomware identification | SecureLink CDC specially crafted rules optimized for this particular threat | CSC 8: Malware Defences | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |

| Name | Description | CIS Critical Security Control | ISO 27002:2014 | PCI-DSS v.3.2 |
|---|---|---|---|---|
| New Installed Malicious Service | Malware often enable persistence by installing themselves as a service. This use case detects suspicious installation of services | CSC 8: Malware Defences | 12.2.1 Controls against malware<br>12.6.2 Restrictions on software installation | 10.2.7 Creation and deletion of system- level objects. |
| Lateral Movement | Attackers use various tools to move across the network with the aim of gaining higher privileges than they have on a compromised machine. This use case attempts to detect such behavior. | CSC 12: Boundary Defence | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| High Probability of Malicious Activity | Malicious actors are using more and more ambitious techniques to deliver payloads to a machine. This use case contains indication of that. | CSC 8: Malware Defences | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| Device Not Conforming to Baseline | This use case attempts to find indications of rogue devices in a customer network. | CSC 12: Boundary Defence | 8.1.1 Inventory of assets | 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. |
| Windows Audit Trail Manipulation | An attacker might attempt to hide his/her action by deleting audit trail from monitored devices. This use case detects aims at detecting such behavior. | CSC 12: Boundary Defence | 12.4.2 Protection of log information | 10.2.3 Access to all audit trails.<br>10.2.6 Initialization, stopping, or pausing of the audit logs.<br>10.5 Secure audit trails so they cannot be altered. |
| Suspicious usage of DNS | DNS can be used for tunneling but it can also pose a risk for clients or servers that do not use the company supplied internal DNS servers. The purpose of this use case is to monitor for these different scenarios. | CSC 12: Boundary Defence<br>CSC 8: Malware Defence | 12.2.1 Controls against malware | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| User Account Not Conforming to Baseline | Looks for authentication anomalies in AD for accounts not conforming to user naming conventions | CSC 12: Boundary Defence<br>CSC 16: Account Monitoring and Control | 9.2.2 User access provisioning | 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. |
| Suspicious Network Activity | Looks for specific attacks in IDS/IPS and sandbox related alerts. | CSC 12: Boundary Defence | | |
| Web Application Attacks | Looks for attacks related to OWASP Top 10 in IIS/ Apache related access logs | CSC 12: Boundary Defence | | |