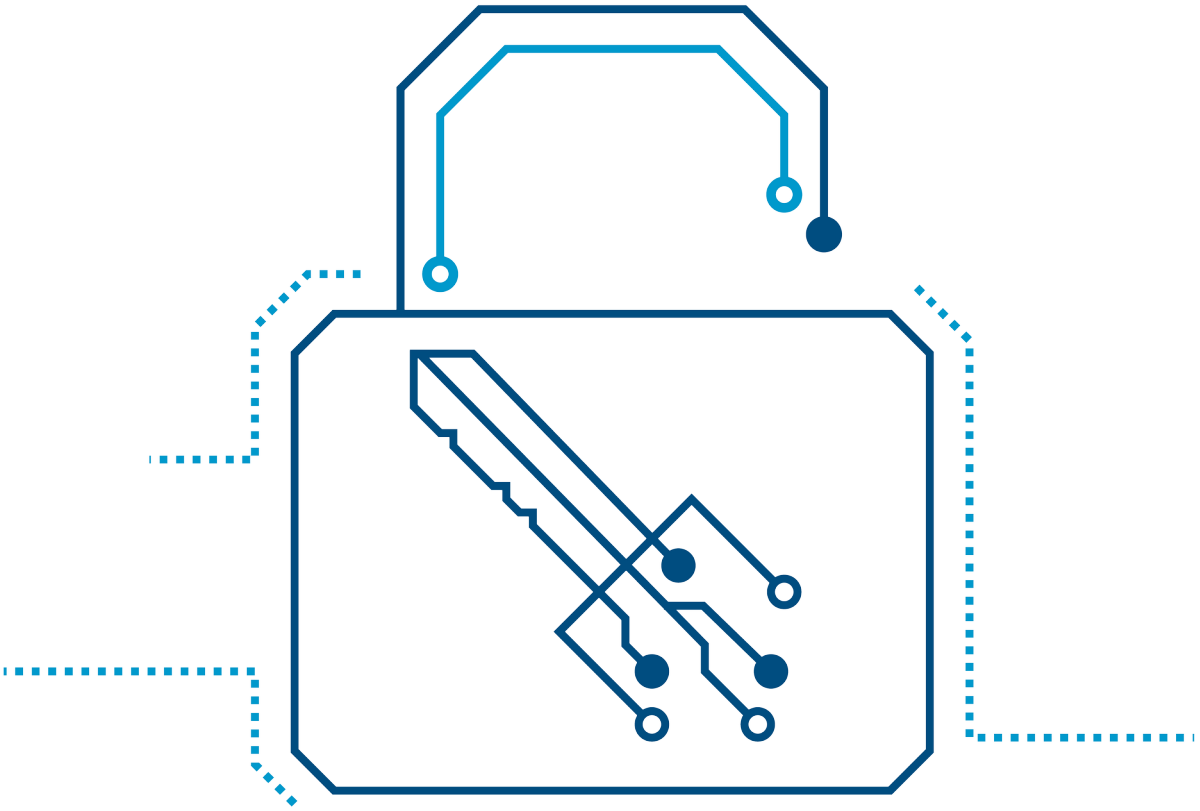
TLP:CLEAR

DFN-CERT

DFN-Security

- Logbasierte Usecases -

Hamburg, 18.03.25



Dieser technische Report wird auf "AS-IS"-Basis vorgelegt. Die DFN-CERT Services GmbH übernimmt keine Gewährleistungen jeglicher Art, weder implizit noch explizit, in Bezug auf jeglichen Sachverhalt oder Inhalt einschließlich, aber nicht darauf beschränkt, Zweckmäßigkeit, Gebrauchstauglichkeit, Ausschließlichkeit oder Folgen aus der Verwendung des Inhaltes. Die DFN-CERT Services GmbH übernimmt keine Gewährleistung jeglicher Art in Bezug auf Patentfreiheit oder Freiheit von Warenzeichen- oder Urheberrechtsverletzungen.

Der Gebrauch von eingetragenen Warenzeichen in diesem Report dient nicht der Absicht, in irgendeiner Art und Weise die Rechte der Inhaber der Warenzeichen einzuschränken oder zu verletzen.

Dokument Informationen

Sperrvermerk	**ohne**
Einstufung nach TLP	TLP:CLEAR
Dateiname	DFN-Security-Logbasierte-Usecases.odt
Letzte Bearbeitung	Dienstag, 18. März 2025
Seitenanzahl	21
URL aktuelle Version	https://www.dfn-cert.de/leistungen/security-operations/
Version	2.0

Inhaltsverzeichnis

1. Einführung

1.1. Ziel dieses Dokuments

Dieses Dokument beschreibt die aktuellen Usecases des DFN-Security- / SOC-Systems, die auf der Verarbeitung eingelieferter Logdaten basieren. Es enthält Informationen darüber, welche Logdaten von den Benutzern des Systems in welchem Format bereitgestellt werden müssen, damit diese Usecases in der Überprüfung aktiv sind.

1.2. Zielgruppe dieses Dokuments

Dieses Dokument wendet sich an Interessierte und Teilnehmer am Dienst DFN-Security, die Logdaten zur Auswertung bereitstellen (wollen), sowohl aus technischer als auch organisatorischer Sicht.

1.3. Grenzen dieses Dokuments

Nachfolgend wird die Architektur des SOC-Systems und der Datenfluss kurz vorgestellt, weitere Erläuterungen finden sich in der Beschreibung des SOC-Connectors. Rechtliche Rahmenbedingungen, die sich z.B. aus Verträgen oder Gesetzen ergeben, werden nicht thematisiert und als bekannt vorausgesetzt.

Logdaten können aus verschiedenen Quellen in das System eingeliefert werden. Dieses Dokument ist beschränkt auf Logdaten, die aus der internen IT-Infrastruktur eines Teilnehmers über eine lokale SOC-Connector- / SOC-Agent-Instanz eingeliefert werden.

1.4. Art dieses Dokuments

Die Usecases können sich im Laufe der Zeit ändern und es werden weitere ergänzt, so dass dieses Dokument ebenfalls ständigen Änderungen unterworfen ist. Aufgrund der kontinuierlichen Bearbeitung zum Erhalt der Aktualität handelt es sich um ein lebendes Dokument.

1.5. Sprachregelung

Dieses Dokument befasst sich ausschließlich mit Komponenten des DFN-Security-Systems, die im Rahmen des Security Operations Projektes im DFN entwickelt werden, so dass im Folgenden auf Prefixe wie „DFN-Security“ und „SOC“ (Security Operations Center) weitestgehend verzichtet wird, sofern es sich nicht um Produktnamen handelt.

1.6. Struktur dieses Dokuments

Das Dokument gliedert sich in folgende Teile:

- Im anschließenden Kapitel wird ein Überblick gegeben, wie die Logdaten von der internen IT-Infrastuktur des Teilnehmers durch das System transferiert werden und daraus möglicherweise Warnmeldungen entstehen.
- Im darauf folgenden Kapitel werden die aktuell implementierten Usecases erläutert. Abschließend werden Usecases beschrieben, die in Vorbereitung sind und für die Feedback erwünscht ist.
- Im Anhang befinden sich Beispiellogzeilen im Syslog-Format

2. Verarbeitung von Logdaten durch das System

Die Logdaten der Teilnehmer werden von dem SOC-Connector bzw. SOC-Agent, der lokal auf den Systemen des Teilnehmers installiert ist, an einen Concentrator-Cluster übertragen. Welche Logdaten übermittelt werden, liegt ganz in Verantwortung des Teilnehmers. Für die Übertragung wird das Kafka-Producer-Protokoll benutzt, das mit TLS-Verschlüsselung und gegenseitiger Zertifikats-basierter Authentifizierung abgesichert ist. Die Daten werden im JSON-Format übertragen.

Der Concentrator-Cluster nimmt eine erste Filterung, Normalisierung und Analyse der eingehenden Daten vor. Dazu gehört z. B. die Identifikation von IP-Adressen im Text der Meldung sowie die Anreicherung des Datensatzes um GeoIP-Daten zu diesen IP-Adressen.

Die Daten werden anschließend an die zentrale Core-Komponente weitergeleitet, wo sie weiter analysiert und ggf. mit weiteren Daten z. B. aus öffentlichen oder proprietären Quellen wie MISP (Malware Information Sharing Platform) angereichert werden. Schließlich erfolgt – wenn nötig – die finale Klassifizierung als sicherheitsrelevanter Vorfall, für den dann eine Automatische Warnmeldung erzeugt wird.

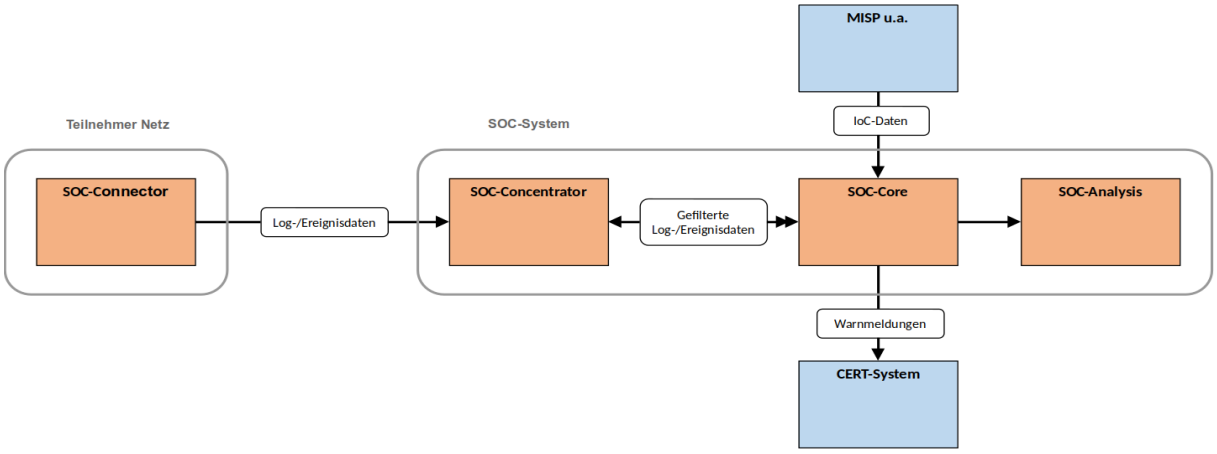


Abbildung 1: SOC-System

Typischerweise durchlaufen die Logdaten diese Verarbeitungsstufen:

- Normalisierung
- Erkennung von IP-Adressen und Anreicherung mit GeoIP-Daten
- Erkennung und Analyse von konkreten Meldungstypen („Usecases“) inklusive der Anwendung spezifischer Filter
- Weitere Anreicherung bzw. Abgleich mit zusätzlichen Daten (z. B. IoC (Indicators of Compromise))
- Aggregation von gleichartigen Meldungen, um die Relevanz zu erhöhen
- Finale Klassifizierung als „sicherheitsrelevanter Vorfall“

Zusätzlich zu dieser automatischen Verarbeitung der Logdaten bietet die Core-Komponente die Möglichkeit, die Daten auch nachträglich manuell mit zusätzlichen Filter- und Aggregationsregeln in der Analyse-Komponente zu untersuchen.

Ereignisse, die als sicherheitsrelevanter Vorfall erkannt wurden und zu denen eine Benachrichtigung erfolgen soll, werden automatisch an andere Systeme der DFN-Security-Infrastruktur übergeben. Zur weiteren Verarbeitungskette gehören interne Applikationen wie das System zur Erzeugung der Automatischen Warnmeldungen und das DFN-Security Portal.

Die Verteilung der analysierten Vorfälle wird über die Einträge (Netzwerkstruktur- / Domainliste des Teilnehmers mit Kontakten) im DFN-Security Portal gesteuert.

3. Beschreibung der Usecases

Zu jedem Usecase sind eine Kurzbeschreibung, die zu übermittelten Logdaten, die Detektionsmethode, der AW-Meldungsbezug sowie weitere Details angegeben. Falls Sie weitere Logdaten von Systemen identifizieren, die auf einen der unten genannten Usecases passen, aber nicht von uns aufgeführt werden, sprechen Sie uns gerne an. Wir versuchen dann, die entsprechenden Regeln umzusetzen. Sollten Sie weitere Usecase-Ideen haben, kommen Sie ebenfalls auf uns zu.

Kontakt zum DFN-CERT bzgl. Usecases: portal-contact@dfn-cert.de

3.1. Syslog-basierte Usecases

Usecases in dieser Kategorie basieren auf Logdaten im Syslog-Format. Dabei werden Systeme identifiziert, die durch verdächtige Verbindungen/Zugriffe, unnormales Verhalten, Bereitstellung von Schadsoftware oder eine Infektion aufgefallen sind.

Die Logdaten werden im Format nach RFC 5424 erwartet und müssen insbesondere den APP-NAME enthalten, da dieser bei der Erkennung für die meisten Usecases verwendet wird. Beispiele für passende APP-NAMEs sind unter „Zu übermittelnde Logdaten“ bei den jeweiligen Usecases aufgeführt. Zudem muss der Zeitstempel in einem mit RFC 5424 konformen Format vorhanden sein und unbedingt die Zeitzone enthalten.

3.1.1. Verdächtige Netzwerkzugriffe

Gesucht werden verdächtige Zugriffe aus einem lokalen Netz heraus auf IP-Adressen (und Ports) bekannter Malware- bzw. Command & Control (C&C, C2)-Server.

Zu übermittelnde Logdaten
- IPTables-basierte Firewall-Logs

Detektion
- Zugriffe auf bekannte Malware- bzw. Command & Control (C&C, C2)-Server

AW-Meldungsbezug
- Kategorie Bot
- Fallback-Domain der Einrichtung

Details
Die IPTables-basierten Firewall-Logs einer Einrichtung werden anhand von Listen bekannter C&C-Server nach verdächtigen Zieladressen durchsucht. Als Diagnose wird die zu den IP-Adressen gehörige Malware geliefert.

3.1.2. Mailversand infizierter Clients

Infizierte Rechner versenden infizierte E-Mails, die von E-Mail-Virenscannern erkannt, geloggt und (ggf.) blockiert werden.

Zu übermittelnde Logdaten
- Amavis-Logs
- APP-NAME = amavis (STARTSWITH)

Detektion
- mit „Blocked INFECTED“ oder „Passed INFECTED“ markierte Meldungen

AW-Meldungsbezug
- Kategorien Attack/Phishing, Attack/Malware
- IP-Adresse der einliefernden Instanz

Details
Zentrale E-Mail-Server verwenden Viren- / Malware-Scanner, um verdächtige E-Mails zu erkennen und ggf. die Weiterleitung zu blockieren. Der Empfänger ist dadurch geschützt. Wenn der Absender zu einem (anderen) Teilnehmer gehört, soll dieser Teilnehmer gewarnt werden, dass ein Rechner innerhalb des eigenen Netzes möglicherweise mit Malware infiziert ist.

Dazu werden die E-Mail-Logs hinsichtlich der Einträge „Blocked INFECTED“ oder „Passed INFECTED“ von Amavis ausgewertet.

Hier werden vier Filter angewendet:

- „exclude_ip_sets“: Wenn die vermeintliche Sender-IP zu einer vorgegebenen Liste von E-Mail-Servern gehört, handelt es sich entweder um einen False Positive oder der tatsächliche Sender kann nicht ermittelt werden. Das Ereignis wird ignoriert.
- „malware_downgrade_to_junk“: Wenn der Malware-Name auf vorgegebene Muster passt, handelt es sich um Junk-Mail und nicht um gefährliche Malware. Das Ereignis wird ignoriert und die Diagnose ist „Junk“.
- „malware_virus_vs_phishing“: Wenn die Länge der E-Mail eine bestimmte Größe unterschreitet, handelt es sich eher um eine Phishing-E-Mail als um gefährliche Malware. Die Diagnose lautet „Phishing“ und die erkannte Phishing-Kampagne wird als Ergebnis gesetzt.
- „malware_infection_email“: Die Diagnose ist „Malware“ und die erkannte Schadsoftware wird als Ergebnis gesetzt.

3.1.3. Wiederholt blockierte Angreifer

Angreifer werden mehrfach nacheinander durch Mechanismen (z. B. fail2ban) geblockt.

Zu übermittelnde Logdaten
- Fail2ban, SSHGuard
- APP-NAME = fail2ban.actions (EQUALS)
- APP-NAME = sshguard (EQUALS)

Detektion
- 3 Bans pro IP und Stunde

AW-Meldungsbezug
- Kategorie Attack/Botlike
- IP-Adresse des Angreifers

Details
Auf vielen Servern laufen Prozesse, die z. B. auf Logmeldungen zu fehlgeschlagenen Login-Versuchen reagieren. Wenn entsprechende Meldungen in kurzer Zeit mehrfach zur gleichen Quell-IP-Adresse

gefunden werden, so wird diese IP-Adresse für einige Minuten geblockt, kann nach Ablauf der Blockade aber wieder Login-Versuche starten.

Wenn mehrere Blockaden zur gleichen IP-Adresse in kurzer Zeit (3 Bans pro IP und Stunde) in Logs gefunden werden (auch für unterschiedliche Dienste oder Server), so handelt es sich möglicherweise um einen Angriffsversuch.

3.1.4. Verdächtige Verbindungsversuche

Angreifer versuchen Verbindungen zu Systemen aufzubauen für die Sie keine Berechtigungen haben.

Zu übermittelnde Logdaten

- Fortigate

Detektion

- abgelehnte Verbindungen auf den Ports TCP/22 und TCP/3389

AW-Meldungsbezug

- Kategorie Attack/Portscan
- IP-Adresse des Angreifers

Details

Auf Firewalls können eingehende Verbindungen auf bestimmten Ports abgelehnt werden, da diese als verdächtig eingestuft werden. Das kann von Angreifern benutzt werden, um offene Ports zu identifizieren bzw. Verbindungen zu Systemen aufzubauen. Interessante Ports sind z. B. TCP/22 und TCP/3389.

3.1.5. Verdächtige DNS-Anfragen

Ein Client im internen Netz versucht, den FQDN eines bekannten bösartigen Servers aufzulösen.

Zu übermittelnde Logdaten

- Bind-Logs mit „umgeleiteten“ Anfragen
- APP-NAME = named (STARTSWITH)

Detektion

- „umgeleitete“ (rewrite) Anfragen

AW-Meldungsbezug

- Kategorien Access/Domains: C2/Malware, Access/Domains: Malicious, Access/Domains: Phishing
- IP-Adresse des DNS-Clients

Details

Die DNS-Server erhalten über DNS-RPZ eine oder mehrere Listen von bekannten bösartigen Domains bzw. Hostnamen. Der DNS-Server liefert daher für solche Anfragen die IP-Adresse eines ungefährlichen Hosts zurück, zu dem der Client dadurch umgeleitet wird. Wurde die Anfrage durch einen Webbrowser gestellt, bekommt der Client eine Landing-Page angezeigt, die den Grund der Umleitung erklärt.

Die konkrete Anfrage wird zwar geblockt, sodass keine unmittelbare Gefahr durch diesen konkreten Zugriff besteht. Aber die Anfrage an sich kann ein Indiz sein, dass der Client mit Malware infiziert ist.

3.1.6. Mailversand mit infizierten Anhängen

Infizierte Rechner versenden E-Mails mit infizierten Anhängen, die von Scanner auf Firewalls erkannt, geloggt und (ggf.) blockiert werden.

Zu übermittelnde Logdaten
- Forcepoint NGFW (File Reputation (McAfee GTI))

Detektion
- mit „File_Malware-Blocked“ und „SMTP“ markierte Meldungen

AW-Meldungsbezug
- Kategorie Attack/Virus
- IP-Adresse des Senders

Details
Firewalls können über verschiedene Mechanismen verdächtige eingehende Datenströme loggen. Darunter sind eingehende E-Mails, deren Anhang als maliziös erkannte wurde.

3.1.7. Verdächtige Logins

Manche Anmeldungen können, obwohl sie erfolgreich waren, aus verschiedenen Gründen verdächtig sein.

Zu übermittelnde Logdaten
- OpenSSH, Pulse Secure
- APP-NAME = sshd (STARTSWITH)
- APP-NAME = PulseSecure (EQUALS)

Detektion
- in kurzen Abständen aufeinanderfolgende Logins aus verschiedenen Ländern

AW-Meldungsbezug
- Kategorie Access/GeoIP
- Fallback-Domain der Einrichtung

Details
Für erfolgreiche z. B. SSH-Logins wird mit Hilfe einer GeoIP-Datenbank aus den Logs von SSH-Servern (OpenSSH) ermittelt, aus welchem Land die IP-Adresse des Clients kommt. Wenn kurz danach ein weiterer (erfolgreicher) Login zum gleichen Benutzernamen und zum gleichen Service, aber aus einem anderen Land erfolgt, so wird das als verdächtig eingestuft.

3.1.8. Fehlverhalten eines Mail-Servers

Ein falsch konfigurierter, veralteter oder kompromittierter E-Mail-Client befolgt das SMTP-Protokoll nicht.

Zu übermittelnde Logdaten
- Postfix-Logs
- APP-NAME = postfix (STARTSWITH)

Detektion
- 1000 Meldungen pro IP innerhalb von 24 Stunden mit „lost connection after“ oder „improper command pipelining after“

AW-Meldungsbezug
- Kategorie Attack/Protocol Error
- IP-Adresse des SMTP-Clients

Details
Zentrale E-Mail-Server (Postfix) protokollieren, wenn sich ein Client (oftmals ein anderer Durchgangsserver) nicht an das SMTP-Protokoll hält (z. B. wird die Verbindung zu früh abgebrochen oder es wird ein unerwartetes Kommando gesendet).

Das kann ein Hinweis auf ein falsch konfigurierten oder veralteten Client sein. Oder aber ein kompromittiertes System versucht Spam in großer Menge zu versenden. Einzelne solcher Meldungen sind in der Regel nicht als sicherheitsrelevant zu werten. Wenn der gleiche Client aber in kurzer Folge viele solcher Meldungen erzeugt, ist zumindest nicht alles in Ordnung.

Entsprechende Meldungen werden erkannt und die IP-Adresse des Clients wird extrahiert. Die Anzahl der Meldungen pro Client-IP und Zeitfenster wird gezählt. Wenn eine bestimmte Schwelle erreicht wird, wird eine Warnmeldung erzeugt.

3.1.9. Bereitstellung von Schadsoftware

Ein System wurde identifiziert, das Schadsoftware (Malware) zum Download bereitstellt.

Zu übermittelnde Logdaten
- Forcepoint NGFW (File Reputation (McAfee GTI))

Detektion
- mit „File_Malware-Blocked“ und „HTTP“ markierte Meldungen

AW-Meldungsbezug
- Kategorie Hosting/Malware
- IP-Adresse des Senders

Details
Firewalls können über verschiedene Mechanismen verdächtige ausgehende Datenströme loggen. Darunter sind Zugriffe auf Webseiten, die Schadsoftware, JavaScript-Code oder andere aktive Web-Inhalte bereitstellen, die bei Besuch der Seite ausgeführt werden.

3.2. Windows-basierte Usecases

In diesem Abschnitt sind Usecases aufgeführt, die auf der Auswertung von Windows Event IDs basieren. Zu beachten ist, dass bei der Einlieferung die XML-Struktur der Events erhalten bleibt.

3.2.1. Änderungen an der Systemüberwachungsrichtlinie

Eine Änderung an der Systemüberwachungsrichtlinie wurde durchgeführt.

Zu übermittelnde Logdaten
- Event ID 4719

Detektion
- jedes Event löst eine Meldung aus

AW-Meldungsbezug
- Kategorie Security Monitoring/System Audit Policy changed
- Fallback-Domain der Einrichtung
- Warnmeldung wird zeitnah verschickt
- nur das erste Event des Tages löst eine AW-Meldung aus

Details
Alle Änderungen an der Systemüberwachungsrichtlinie werden geloggt. Jede Änderung löst ein Event aus. Inhalt des Events sind: Zeitstempel, Verursacher der Änderung, geänderte Audit-Kategorie und -Subkategorie. Änderungen an der Systemüberwachungsrichtlinie können ein Hinweis auf Verschleierung von Angriffen sein. Prüfen Sie jede ungeplante Änderung.

Die Überwachung von Richtlinienänderungen gehört zu den grundlegenden Sicherheitsüberwachungsrichtlinien:

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/security-auditing-overview

Sie können diese Sicherheitseinstellung konfigurieren unter: "Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie"

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/basic-audit-policy-change

Weitere Informationen zur Windows Event ID 4719:

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/event-4719

3.2.2. Überwachungsprotokoll wurde gelöscht

Das Überwachungsprotokoll eines Windows-Systems wurde gelöscht.

Zu übermittelnde Logdaten
- Event ID 1102

Detektion
- jedes Event löst eine Meldung aus

AW-Meldungsbezug
- Kategorie Security Monitoring/Audit Log cleared
- Fallback-Domain der Einrichtung
- Warnmeldung wird zeitnah verschickt

Details
Üblicherweise ist es nicht erforderlich, das Überwachungsprotokoll manuell zu löschen. Jede Änderung löst ein Events aus. Inhalt des Events sind: Zeitstempel, Verursacher der Änderung, betroffenes System. Das Löschen des Überwachungsprotokoll kann ein Hinweis auf Verschleierung von Angriffen sein. Prüfen Sie jede ungeplante Änderung.

Weitere Informationen zur Windows Event ID 1102:

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/event-1102

3.2.3. Fehlgeschlagene Anmeldeversuche

Für einen Windows-Account wurden innerhalb einer Stunde mehrere fehlgeschlagene Anmeldeversuche von derselben IP-Adresse detektiert.

Detektion
- 50 fehlgeschlagene Anmeldeversuche von derselben IP-Adresse innerhalb einer Stunde

AW-Meldungsbezug
- Kategorie Security Monitoring/Account Logon failed
- Fallback-Domain der Einrichtung

Details
Fehlgeschlagene Anmeldeversuche können ein Hinweis auf einen Angreifer sein. Inhalt der Meldung sind: Zeitstempel, Verursacher der Änderung, betroffenes System. Das massivesAuftreten solcher Events kann auf Konfigurationsfehler hindeuten, bspw. wenn die TLS-Konfiguration nicht für alle Server und Clients konsistent ist.

Weitere Informationen zur Windows Event ID 4625:

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/event-4625

3.2.4. Änderung des Administratorkennworts des Directory Services Restore Mode (DSRM)

Das Administratorkennworts des Directory Services Restore Mode (DSRM) wurde geändert.

Zu übermittelnde Logdaten
- Event ID 4794

Detektion
- jedes Event löst eine Meldung aus

AW-Meldungsbezug
- Kategorie Security Monitoring/DSRM Administrator Password set
- Fallback-Domain der Einrichtung
- Warnmeldung wird zeitnah verschickt

Details
Die Änderung des Administratorkennworts des Directory Services Restore Mode (DSRM) sollte geloggt werden. Dieses Event tritt nur auf Domain Controllern auf. Jede Änderung löst ein Event aus. Inhalt desr Events sind: Zeitstempel, Verursacher der Änderung, betroffenes System.

Der Verzeichnisdienst-Wiederherstellungsmodus (DSRM) ist ein spezieller Bootmodus für die Reparatur oder Wiederherstellung von Active Directory. Er wird verwendet, um sich am System anzumelden, wenn ein Active Directory ausgefallen ist oder wiederhergestellt werden muss. Eine Änderung des Passworts kann den Zugriff auf den DSRM verhindern.

Hinweise für das Zurücksetzen des Administratorkontokennworts für den Verzeichnisdienst-Wiederherstellungsmodus in Windows Server finden Sie hier:

https://learn.microsoft.com/de-de/troubleshoot/windows-server/identity/reset-directory-services-restore-mode-admin-pwd

Weitere Informationen zur Windows Event ID 4794:

https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/event-4794

3.3. Usecases in Vorbereitung

Die Usecases in diesem Abschnitt sind technisch vorbereitet. Die letztliche Aktivierung erfordert aber Hinweise von Nutzenden. Wenden Sie sich dazu an portal-contact@dfn-cert.de.

3.3.1. Installation eines Dienstes

Ein neu installierter Dienst wurde als bösartig erkannt.

Zu übermittelnde Logdaten
- Event ID 4697

Detektion
- das Feld 'ServiceName' wird gegen Listen mit bösartigen Windows Servicenamen abgeglichen

AW-Meldungsbezug
- Kategorie Security Monitoring/Service installed
- Fallback-Domain der Einrichtung
- Warnmeldung wird zeitnah verschickt

Details
Die Installation eines neuen Dienstes auf wichtigen Systemen sollte geloggt werden. Da Windows-Systeme automatisiert neue Dienste installieren, kann nicht jedes Auftreten dieses Events eine Meldung auslösen.

Weitere Informationen zur Windows Event ID 4697:

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4697

Feedback erbeten
Wir freuen uns über Listen zum Abgleich.

3.3.2. Geplante Aufgabe erstellt/aktualisiert

Eine neu erstellte oder aktualisierte Aufgabe wurde als bösartig erkannt. Die Aufgabe wurde mit unsicheren Optionen erstellt/aktualisiert.

Zu übermittelnde Logdaten

- Event IDs 4698 und 4702

Detektion

- das Feld 'TaskName' wird gegen Listen mit bösartigen Windows Servicenamen abgeglichen
- unterhalb von 'TaskContent' wird das Feld 'LogonType' auf '<LogonType>Password</LogonType>' geprüft

AW-Meldungsbezug

- Kategorie Security Monitoring/Tast created - updated
- Fallback-Domain der Einrichtung
- Warnmeldung wird zeitnah verschickt

Details

Alle geplanten aktualisierten bzw. neu erstellten Aufgaben, die sich im Stammknoten unter Task Scheduler Library befinden, sollten überwacht werden. Geplante Aufgaben werden häufig von Schadsoftware verwendet, um auch nach einem Neustart weiter Zugriff auf ein System zu haben oder andere schädliche Aktionen durchzuführen. Enthält das Feld 'LogonType' den Wert 'Password ' wird das Passwort im Klartext im Credential Manager gespeichert. Da Windows-Systeme bzw. Dienste automatisiert Aufgaben erstellen bzw. aktualisieren, kann nicht jedes Auftreten dieser Events eine Meldung auslösen.

Weitere Informationen zu den Windows Event IDs 4698 und 4702:

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4702

Feedback erbeten

Wir freuen uns über Listen zum Abgleich.

4. Versionshistorie

Datum	Autor	Kommentar	Versionsnummer
13.04.2023	Dieter Stolte	Initiales Dokument	1.0
13.10.2023	Sascha Kriebitzsch	Aktualisierung der Usecases	1.3
18.03.2025	Sascha Kriebitzsch	Neues Layout, Weitere Usecases ergänzt	2.0

Anhang - Logbeispiele

In diesem Abschnitt sind Beispieldaten für die Syslog-basierten Usecases im Format RFC 5424 aufgeführt. Wichtige Felder für die Detektion sind hervorgehoben.

Verdächtige Netzwerkzugriffe

firewall/packet_filter_ulogd

```
<30>1 2025-03-03T13:37:00+01:00 172.16.0.2/172.16.0.2 2025 - - -
03:03-13:37:00 dfn ulogd[25587]: id="2002" severity="info" sys="SecureNet"
sub="packetfilter" name="Packet accepted" action="accept" fwrule="1"
initf="lag1.30" outitf="lag1.5" srcmac="00:11:22:aa:bb:33"
dstmac="00:44:55:cc:dd:66" srcip="194.113.208.66" dstip="194.113.208.67"
proto="6" length="52" tos="0x02" prec="0x00" ttl="127" srcport="57577"
dstport="80" tcpflags="SYN"
```

Mailversand infizierter Clients

amavis/found_infected

```
<21>1 2025-03-03T13:37:00+01:00 mgw-dfn amavis-230-2 4153767 - - (230-2-19)
Blocked INFECTED (MiscreantPunch.EvilMacro.PVDISABLE.170819.UNOFFICIAL)
{RejectedOutbound}, 230-2/MYNETS LOCAL [194.113.208.66] [194.113.208.66]
<max.mustermann@dfn-cert.de> -> <empfaenger@dfn.de>, Queue-ID: AA22222222,
Message-ID: <00000000000000000000000@dfn-cert.de>, mail_id: Di23hJu4578M,
Hits: -, size: 988888, 20000 ms, Scanners: [ClamAV], Viruses:
[MiscreantPunch.EvilMacro.PVDISABLE.170819.UNOFFICIAL], helo: server.dfn-
cert.de, From: "Mustermann, Max"_<max.mustermann@dfn-cert.de>
```

Wiederholt blockierte Angreifer

fail2ban-server/banned

```
<29>1 2025-03-03T13:37:00+01:00 srv-dfn fail2ban.actions 8143 - - NOTICE
[postfix-gateways-soft] Ban 194.113.208.66
```

sshguard/blocked

```
<38>1 2025-03-03T13:37:00+01:00 srv-dfn sshguard 1014 - - Blocking
"194.113.208.66/32" for 960 secs (3 attacks in 2 secs, after 4 abuses over
1266 secs.)
```

Verdächtige Verbindungsversuche

fortigate/denied

```
<189>1 2025-03-03T13:37:00+01:00 FGFW - - - - eventtime=1741011399454290137
tz="+0100" logid="0000000001" type="traffic" subtype="forward"
level="notice" vd="Internet" srcip=194.113.208.66 srcport=33733
srcintf="x3" srcintfrole="wan" dstip=194.113.208.67 dstport=22
dstintf="Internet" dstintfrole="undefined" srccountry="Germany"
dstcountry="Germany" sessionid=1086384265 proto=6 action="deny" policyid=0
policytype="policy" service="SSH-Services" trandisp="noop" duration=0
sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" crscore=30
craction=131072 crlevel="high"
```

Verdächtige DNS-Anfragen

dns/domain-blocked

```
<190>1 2025-03-03T13:37:00+01:00 srv.dfn-cert.de named 1227382 - -  03-
Mar-2025 13:37:00.980 rpz: info: client @0x7t7e0d618ac0  #64772
(deb.debian.org): rpz QNAME CNAME rewrite deb.debian.org/A/IN via
deb.debian.org.zone.community.rpz.dfn.de (CNAME to: landingpage-
misc.security.dfn.de)
```

Mailversand mit infizierten Anhängen

firewall/found_infected_incoming

```
<6>1 2025-03-03T13:37:00+01:00 server.dfn-cert.de "2025-03-03 - - -
13:37:00","93109","194.113.208.66","File
Filtering","Notification",,"Terminate","6","194.113.208.66","194.113.208.6
7","36244","25","2124155.0",,,,,,"1","SMTP","System
alert",,,,,,,,,,,"fw",,,,,"2025-03-03 13:37:00","Firewall","File_Malware-
Blocked",,"Critical","7302330578959963117",,,,,,,,"2ee8738b847bfa2372cd78bb
350d7665","evil.gz",
```

Verdächtige Logins

login/username_ip/sshd2

```
<38>1 2025-03-03T13:37:00+01:00 server.dfn-cert.de sshd 2051029 - -
Accepted publickey for username from 194.113.208.66 port 57112 ssh2: RSA
SHA256:3yymWqv59x7u1O5NKzkdXpHizcjzBEXxUXJzKXexxxx
```

login/username_ip/pulsesecure

```
<134>1 2025-03-03T13:37:00+01:00 server.dfn-cert.de PulseSecure: - - -
2025-03-03 13:37:00 - vpn - [194.113.208.66] test(Studierende)[Studierende]
[eaasdsd3435] - VPN Tunneling: Session started for user  (session:
sidee7118eb9c970c253fd36f06865) with IPv4 address 172.29.0.176, hostname
DESKTOP-1111
```

Fehlverhalten eines Mail-Servers

smtpd/lost_connection

```
<22>1 2025-03-03T13:37:00+01:00 srv-dfn postfix-239-1/smtpd 2482702 - -
lost connection after RCPT from unknown[194.113.208.66]:62472
```

smtpd/improper_command_pipelining

```
<22>1 2025-03-03T13:37:00+01:00 srv-dfn postfix-172-2/smtpd 3587772 - -
improper command pipelining after RSET from
server.org[194.113.208.66]:33764: QUIT\r\n
```

Bereitstellung von Schadsoftware

firewall/found_infected_outgoing

```
<6>1 2025-03-03T13:37:00+01:00 server.dfn-cert.de "2025-03-03 - - -
13:37:00","55836","192.168.0.100","File
Filtering","Notification",,"Terminate","6","194.113.208.66","194.113.208.6
7","53074","80","2102044.5",,,,,,"2","HTTP","System
alert",,,,,,,,,,,,"fw",,,,,"2025-03-03 13:37:00","Firewall","File_Malware-
Blocked",,"Critical","7302340998491397",,,,,,,"http://evil.com/download/
evil.exe","a2c054f1c7b93df24260c3176f33","evil.exe",
```