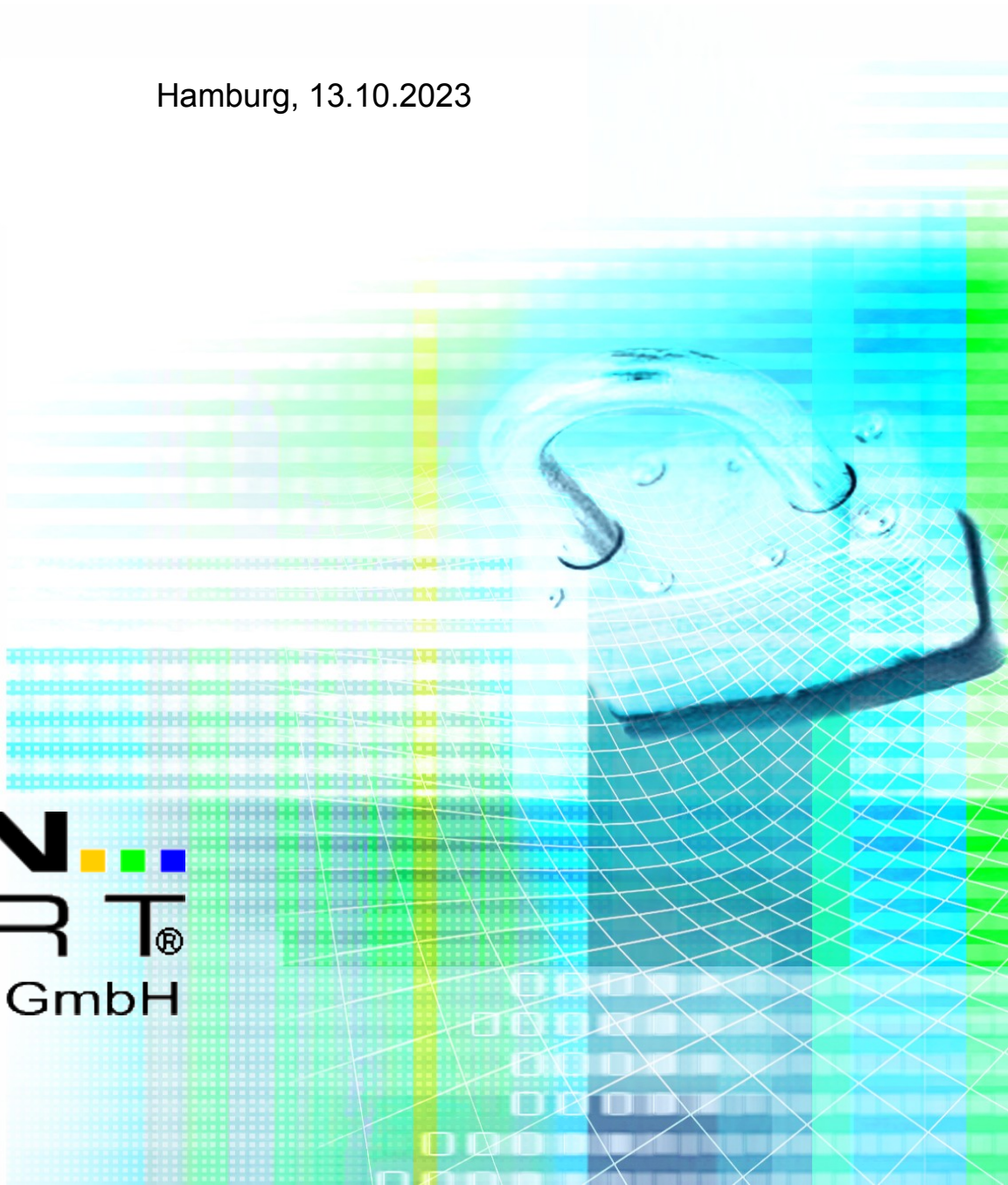
DFN.Security

- Logbasierte Usecases -

Hamburg, 13.10.2023



DFN-CERT® Services GmbH

Dokument-Informationen	
Sperrvermerk	Nur für: DFN-CERT Services GmbH, DFN-Verein, Teilnehmer und Interessierte am Dienst DFN.Security
Dateiname	DFN.Security-Logbasierte.Usecases.odt
letzte Bearbeitung	Freitag, 13. Oktober 2023
Seitenanzahl	13
URL aktuelle Version	https://www.dfn-cert.de/leistungen/secops.html

Inhaltsverzeichnis

Abbildungsverzeichnis

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.

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.

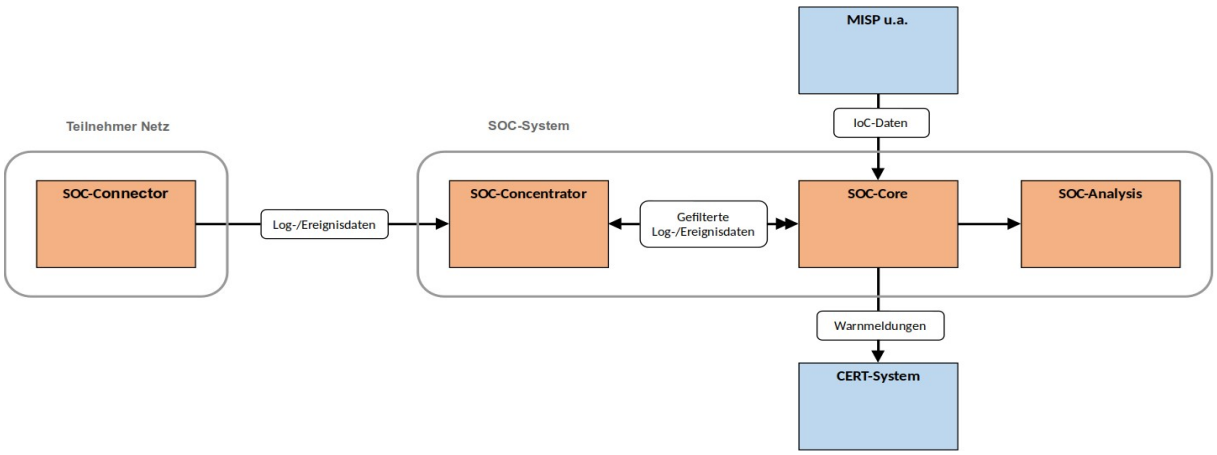


Abbildung 1: SOC-System

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

3.1 Kompromittierte Clients im X-WIN

Eine Warnmeldung wird an den Administrator auffälliger Clients gesendet, falls verdächtige Netzwerkzugriffe oder eine Infektion erkannt werden.

3.1.1 Usecase firewall/packet_filter_ulogd

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

Die IPTables-basierten Firewall-Logs einer Einrichtung werden dazu nach verdächtigen Zieladressen anhand von Listen bekannter C&C-Server durchsucht. Der benutzte Filter ist „packet_filter_ioc_match“ und liefert als Diagnose die erkannte Malware.

Der Hostname des Servers, der die Logs eingeliefert hat, wird über die Datenbank des DFN.Security-Portals für Domainkontakt verwendet, um die Empfänger der Warnmeldung zu bestimmen.

3.1.2 Usecase amavis/found_infected

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

Zentrale E-Mail-Server verwenden Antiviren-/Antimalware-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.

Die IP-Adresse der einliefernden Instanz wird verwendet, um den Teilnehmer zu identifizieren, der benachrichtigt werden soll.

Aktuell werden auch Vorfälle an das System für die Automatischen Warnmeldungen gesendet, bei denen die IP-Adresse nicht zu einem Teilnehmer gehört, im Rahmen des Datenaustausch mit anderen CERTs.

3.1.3 Usecase fail2ban-server/banned

Angreifer werden mehrfach nacheinander durch fail2ban geblockt.

Auf vielen Servern laufen fail2ban-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 fail2ban-Logs gefunden werden (auch für unterschiedliche Dienste oder Server), so handelt es sich möglicherweise um einen Angriffsversuch.

Die IP-Adresse des Angreifers wird verwendet, um einen Ansprechpartner innerhalb des X-WiN zu bestimmen.

3.1.4 Usecase dns/domain-blocked

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

Die DNS-Server erhalten über DNS-RPZ eine oder mehrere Listen von bekannten, bösartigen Domains bzw. Hostnamen. Der Versuch, so einen Hostnamen aufzulösen, kann nicht gut sein. Der DNS-Server liefert daher für diese Anfragen eine "falsche" IP-Adresse zurück, die auf eine extra vorbereitete, ungefährliche Landing-Page verweist.

Die konkrete Anfrage wurde 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.

Die IP-Adresse des DNS-Clients wird verwendet, um die Einrichtung und den zuständigen Ansprechpartner zu bestimmen.

3.2 Angreifer von außen

Eine Warnmeldung wird an den Administrator eines angegriffenen Servers gesendet.

3.2.1 Usecase login/username_ip/sshd2

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

Für erfolgreiche 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. Dafür wird der Filter „suspicious_login_geoip“ benutzt.

Der Hostname des Servers, der den erfolgreichen Login protokolliert hat, wird über die Datenbank der geprüften Domains verwendet, um den Empfänger der Warnmeldung zu finden. Das impliziert, dass der Hostname in der Syslog-Zeile vollständig qualifiziert ist!

3.3 Auffälliger Server im X-WiN

Eine Warnmeldung wird an den Administrator des auffälligen Systems gesendet.

3.3.1 Usecase smtpd/improper_command_pipelining bzw. smtpd/lost_connection

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

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 i.d.R. 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.

Die Usecases smtpd/lost_connection und smtpd/improper_command_pipelining werden gemeinsam aggregiert in „mailserver/protocol_error“.

Die Schwellwerte für Meldungen pro IP innerhalb von 24 Stunden sind

- 100: „moderate“
- 1000: „high“

- 10000: „extremely high“

Als Filter wird „aggregation_severity_high“ verwendet, der eine Warnung ab dem Schwellwert „high“ erzeugt.

Die IP-Adresse des SMTP-Clients wird verwendet, um einen Ansprechpartner innerhalb des X-WiN zu bestimmen.

3.4 Windows Events

Eine Warnmeldung wird an den Administrator des auffälligen Systems oder an die Verantwortlichen der für die Einrichtungen konfigurierten Fallback-Domains gesendet.

3.4.1 Usecase Security Monitoring/System Audit Policy changed

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

Die Überwachung von Richtlinienänderungen gehört zu den grundlegenden Sicherheits-überwachungsrichtlinien:

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

Diese Meldung basiert auf Windows EventID 4719:

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

Da hier keine Adressinformationen vorhanden sind, erfolgt die Zuordnung dieser Warnmeldung auf Grundlage der für die Einrichtungen konfigurierten Fallback-Domains.

3.4.2 Usecase Security Monitoring/Audit Log cleared

Das Überwachungsprotokoll eines Windows-Systems wurde gelöscht. Üblicherweise ist es nicht erforderlich, dieses Protokoll manuell zu löschen. Jede Änderung löst eine Meldung aus. Inhalt der Meldung sind: Zeitstempel, Verursacher der Änderung, betroffenes System. Das

Löschen des Überwachungsprotokoll kann ein Hinweis auf Verschleierung von Angriffen sein. Prüfen Sie jede ungeplante Änderung.

Diese Meldung basiert auf Windows EventID 1102:

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

Da hier keine Adressinformationen vorhanden sind, erfolgt die Zuordnung dieser Warnmeldung auf Grundlage der für die Einrichtungen konfigurierten Fallback-Domains.

3.4.3 Usecase Security Monitoring/Account Logon failed

Für einen Windows-Account wurden innerhalb einer Stunde 10 fehlgeschlagene Anmeldeversuche von derselben IP-Adresse detektiert. Inhalt der Meldung sind: Zeitstempel, Verursacher der Änderung, betroffenes System. Fehlgeschlagene Anmeldeversuche können ein Hinweis auf einen Angreifer sein.

Diese Meldung basiert auf Windows EventID 4625:

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

3.4.4 Usecase Security Monitoring/DSRM Administrator Password set

Die Änderung des Administratorkennworts des Directory Services Restore Mode (DSRM) sollte geloggt werden. Dieses Event tritt nur auf Domain Controllern auf. Jede Änderung löst eine Meldung aus. Inhalt der Meldung 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

Diese Meldung basiert auf Windows EventID 4794:

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

Da hier keine Adressinformationen vorhanden sind, erfolgt die Zuordnung dieser Warnmeldung auf Grundlage der für die Einrichtungen konfigurierten Fallback-Domains.

