

MACMON NAC WHITEPAPER

Integration of macmon NAC with CLEARER

Contents

Introduction 3

Use Cases 3

 Detection of vulnerabilities in endpoints..... 3

 Transfer of endpoints..... 3

Configuration of CLEARER 4

Configuration of macmon NAC 7

Contact DECOIT GmbH 7

Introduction

The desire to offer customers independent IT consulting was the basis for the foundation of DECOIT® GmbH in 2001. To this day, manufacturer neutrality and objectivity are still part of the honest advice given to its customers. Today, the mission of DECOIT® GmbH is to provide, optimize, secure and support technical IT infrastructure and to develop customer-oriented and innovative software solutions. Among employees they cultivate open exchange with short communication paths.

The CLEARER product was developed from the research project of the same name, which aimed at the fulfilment of compliance requirements by automated processing of IT security incidents for small and medium-sized enterprises (SME). To be able to use the full functionality of CLEARER, the connection to macmon NAC is provided. These are monitoring systems with a focus on IT security, which is why various event messages (alarms) from different data sources (firewall logs, database logs, intrusion detection systems) are collected and consolidated.

Use Cases

Viruses and malware can make an administrator's life difficult. If, despite all precautions, such malicious software infects an endpoint, the isolation of this device from the network segment must be done as quickly as possible. This prevents malware from spreading over the network and infecting other resources on the network. CLEARER from DECOIT® GmbH is able to detect such a threat quickly. In CLEARER, detected threats or anomalies are logged in the form of incidents and passed on to macmon NAC on demand. The combination of CLEARER and macmon NAC is a powerful combination of threat detection and isolation of affected endpoints.

Detection of vulnerabilities in endpoints

CLEARER derives a compliance decision from the collected information and enforces it in the company network with the help of macmon NAC. For example, CLEARER sets the compliance status "non-compliant" for an end device that does not comply with the company policies. Using a preset rule, CLEARER isolates an end device by moving it into the remediation VLAN or by switching off the network connection at the switch. In the compliance report, macmon's Web GUI contains a detailed overview of the reasons for which the respective end devices were isolated. In the SIEM-GUI of CLEARER, on the other hand, the incident can be read in detail and a recommendation for action can be found.

Transfer of endpoints

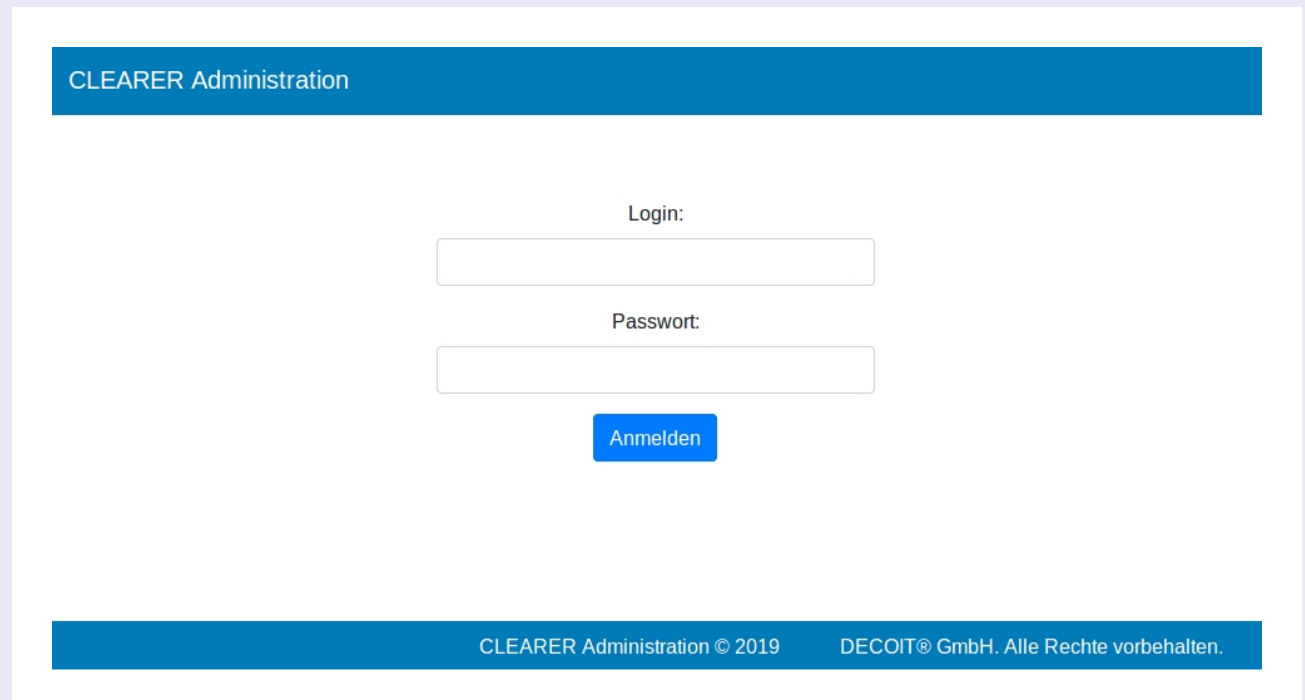
CLEARER collects information about end devices in the company network. At regular intervals, it also queries macmon NAC's database of end devices and thus completes its own overview of all end devices in order to provide optimal protection. Because in the detected incidents CLEARER has to distinguish between known and unknown end devices in order to be able to detect anomalies reliably. With the SIEM-GUI, the security risk of the company can always be identified at a glance or whether the responsible IT administrator should intervene.

Configuration of CLEARER

The installation and configuration of CLEARER is included in the application documentation that is delivered with the system. This consists of the software installation, setup and functional description.

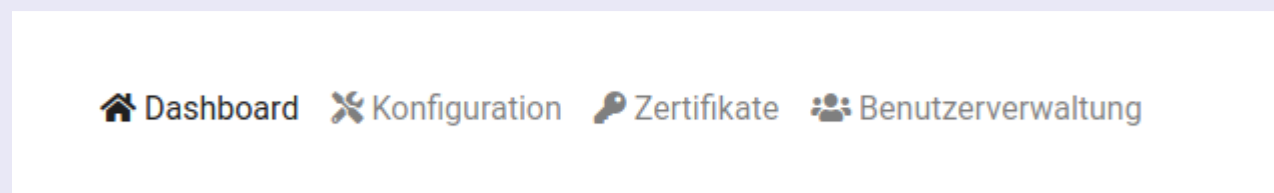
The configuration steps that are specific to macmon are highlighted below:

1. After accessing the CLEARER management interface, you can log in with the user name root and the previously generated password.



The screenshot shows the 'CLEARER Administration' login page. It features a blue header bar with the text 'CLEARER Administration'. Below the header, there is a login form with two input fields: 'Login:' and 'Passwort:'. A blue button labeled 'Anmelden' is positioned below the password field. At the bottom of the page, a blue footer bar contains the text 'CLEARER Administration © 2019' and 'DECOIT® GmbH. Alle Rechte vorbehalten.'

2. The configuration for the components can be accessed via the upper tab. The configuration is divided into six categories. The categories do not correspond to the individual components, but are structured by content. In order to configure a component, changes in several categories may be necessary. Click on *Konfiguration (Configuration)*.



3. Then click on the *Verbindungen (Connections)* tile. The *Verbindungen* category contains the configurations for the connections.

CLEARER Administration Angemeldet als glacier [Abmelden](#)

[Dashboard](#) [Konfiguration](#) [Zertifikate](#) [Benutzerverwaltung](#)

Konfigurationsverwaltung

Verbindungen

[Abbruch und zurück](#) [Speichern](#)

Interner SIEM-GUI Server Port: *
(Standard: 7200)

SIEM-GUI SSL erzwingen: *
Einstellung erzwingt die verschlüsselte Nutzung im Web-Interface der SIEM-GUI (Standard: true)

SIEM-GUI Queue TLS erzwingen: *
Einstellung erzwingt die verschlüsselte Datenabholung aus der Queue (Standard: true)

MacMon IP: *
Für den Anschluss an das macmon System wird die IP Adresse des macmon Systems benötigt. Unter dieser IP Adresse muss die macmon Konfigurations GUI erreichbar sein.

Macmon Benutzer: *
Für das Auslesen und das Durchsetzen der Compliance wird ein aktiver Benutzer auf dem macmon System benötigt.

Benutzername *	<input type="text" value="admin"/>	Passwort *	<input type="password" value="*****"/>
----------------	------------------------------------	------------	--

Rabbit-MQ Host-IP: *
Standardmäßig läuft die Rabbitmq auf dem gleichen Host, wie das restliche System. Es ist auch unwahrscheinlich, dass dies geändert werden muss. (Standard: 127.0.0.1)

CLEARER Administration © 2019 DECOIT® GmbH. Alle Rechte vorbehalten.

- Here you can store the login data for the macmon instance. If these data are missing, IP addresses cannot be resolved to MAC addresses and it is not possible to take action directly from the SIEM-GUI.

MacMon IP: *
Für den Anschluss an das macmon System wird die IP Adresse des macmon Systems benötigt. Unter dieser IP Adresse muss die macmon Konfigurations GUI erreichbar sein.

Macmon Benutzer: *
Für das Auslesen und das Durchsetzen der Compliance wird ein aktiver Benutzer auf dem macmon System benötigt.

Benutzername *	<input type="text" value="admin"/>	Passwort *	<input type="password" value="*****"/>
----------------	------------------------------------	------------	--

- In the *Scenario (Szenarien)* category, the parameters and rules for the two active scenarios can be defined. Here you can also define which networks Zeek should monitor and at which network interface it should listen. An incident for a rule violation will only be created if the IP address or network is located in the areas defined for Zeek to monitor, otherwise the information will already be discarded at Zeek and will never reach the analysis component.

Netzwerk Überwachungs Szenario: *

Überwachung der Kommunikationsbeziehungen im Netzwerk

(Standard: true)

Szenario aktivieren * ☐ true

Die Systeme sind in macmon in Gruppen unterteilt. Alle Systeme der hier eingegebenen Gruppen sollen als PC verwertet werden. ⓘ

macmon PC Gruppen:*

-



Die Systeme sind in macmon in Gruppen unterteilt. Alle Systeme der hier eingegebenen Gruppen sollen als Server verwertet werden. ⓘ

macmon Server Gruppen:*

-



Wenn ein PC als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Bedrohungsstufe. Werte zwischen 1 und 10, eine größere Zahl gibt ein größeres Risiko vor. (Standard: 4)

Bedrohungslevel für PCs * 4

Wenn ein PC als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Priorität. Werte zwischen 1 und 10, eine größere Zahl gibt eine größere Priorität vor. (Standard: 4)

Priorität für PCs * 4

Wenn ein Server als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Bedrohungsstufe. Werte zwischen 1 und 10, eine größere Zahl gibt ein größeres Risiko vor. (Standard: 8)

Bedrohungslevel für Server * 8

Wenn ein Server als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Priorität. Werte zwischen 1 und 10, eine größere Zahl gibt eine größere Priorität vor. (Standard: 8)

Priorität für Server * 8

Wenn ein unbekanntes Gerät als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Bedrohungsstufe. Werte zwischen 1 und 10, eine größere Zahl gibt ein größeres Risiko vor. (Standard: 10)

Bedrohungslevel unbekannter Geräte * 10

Wenn ein unbekanntes Gerät als Quelle des nicht erlaubten Verkehrs ausgemacht wird, gilt diese Priorität. Werte zwischen 1 und 10, eine größere Zahl gibt eine größere Priorität vor. (Standard: 10)

Priorität unbekannter Geräte * 10

IP-Adressen und zeitabhängige Datenverkehr Vorgaben:*

- Here you can differentiate between workstations and servers using macmon groups, and you can also define individual threat levels to enable a better risk assessment later on.

IP-Adressen und zeitabhängige Datenverkehr Vorgaben:*

Die erste Stufe der Überwachung ist eine IP Adressen spezifische Einrichtung der zu überwachenden Zeitbereiche mit Quell- und Ziel-IP.

Benötigt wird eine vollständige IP Adresse (z.B. 192.168.1.10)

Quell-IP-Adresse

Benötigt wird eine vollständige IP Adresse (z.B. 192.168.1.10)

Ziel-IP-Adresse

Erlaubte Zeiten:

Datenverkehr ist zu diesen Zeiten erlaubt. Mehrfache Einträge sind möglich, sich überschneidende Zeiten sind ebenfalls möglich.

Betroffene(r) Tag/Tage *

Jeden Tag

Zeitspanne:*

Die Zeitspanne kann von 00:00 bis 23:59 in 5 Minuten Schritten durch den Regler eingestellt werden

00:00 - 00:00



Gesperpte Zeiten:

Datenverkehr ist zu diesen Zeiten verboten. Mehrfache Einträge sind möglich, sich überschneidende Zeiten sind ebenfalls möglich.

Betroffene(r) Tag/Tage *

Jeden Tag

Zeitspanne:*

Die Zeitspanne kann von 00:00 bis 23:59 in 5 Minuten Schritten durch den Regler eingestellt werden

00:00 - 00:00



- Complete the configuration.

Configuration of macmon NAC

There is no need to configure macmon NAC separately. The exchange between both systems is done via the Rest API or macutil interface. A NAC actuator has been integrated into CLEARER for this purpose.

Contact DECOIT GmbH

Prof. Dr. Kai-Oliver Detken (Sales)

Email: detken@decoit.de

Tel.: 0421-596064-0

Fax: 0421-596064-09

Timo Klecker (Development)

Email: klecker@decoit.de

Tel.: 0421-596064-0

Fax: 0421-596064-09

Henrik Gießel (Engineering)

Email: giessel@decoit.de

Tel.: 0421-596064-0

Fax: 0421-596064-09

Contact

macmon secure GmbH

Alte Jakobstrasse 79-80 | 10179 Berlin

Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu