DECOIT®

macmon
nac intelligent einfach

MACMON NAC WHITEPAPER

Integration von macmon NAC mit CLEARER

Inhaltsverzeichnis

Version: 1.2_de

Einleitung

Der Wunsch, Kunden unabhängige IT-Beratung anzubieten, bildete 2001 die Gründungsgrundlage der DECOIT® GmbH. Bis heute gehört Herstellerneutralität und Objektivität zur ehrlichen Beratung ihrer Kunden. Die Mission der DECOIT® GmbH ist heute die Bereitstellung, Optimierung, Absicherung und der Support von technischer IT-Infrastruktur sowie die Entwicklung kundenorientierter und innovativer Software-Lösungen. Unter Mitarbeitern pflegen sie offenen Austausch mit kurzen Kommunikationswegen.

Das CLEARER-Produkt entstand aus dem gleichnamigen Forschungsprojekt, welches auf die Erfüllung von Compliance-Anforderungen durch automatisierte Bearbeitung von IT-Sicherheitsvorfällen für Klein- und Mittelständische Unternehmen (KMU) abzielte. Um die volle Funktionalität von CLEARER nutzen zu können, ist die Anbindung an das macmon NAC vorgesehen. Es handelt es sich um Monitoring-Systeme mit dem Fokus auf die IT-Sicherheit, weshalb diverse Ereignismeldungen (Alarme) aus verschiedenen Datenquellen (Firewall-Logs, Datenbank-Logs, Intrusion-Detection-Systemen) gesammelt und zusammengeführt werden.

Anwendungsfälle

Viren und Schadsoftware können das Leben eines Administrators schwer machen. Wenn eine solche schädliche Software trotz aller Vorsichtsmaßnahmen ein Endgerät infiziert, muss die Isolierung dieses Endgeräts aus dem Netzwerksegment so schnell wie möglich erfolgen. Dadurch wird verhindert, dass sich eine Schadsoftware über das Netzwerk verbreitet und andere im Netzwerk befindlichen Ressourcen infiziert. CLEARER von der DECOIT® GmbH ist in der Lage, eine solche Bedrohung schnell zu erkennen. In CLEARER werden gefundene Bedrohungen oder Unregelmäßigkeiten in Form von Incidents (Vorfällen) festgehalten und auf Wunsch an macmon NAC übertragen. Die Kombination aus CLEARER und macmon NAC ist eine leistungsstarke Kombination aus Erkennung von Bedrohungen und Isolation von betroffenen Endgeräten.

Erkennung von Schwachstellen in Endgeräten

Aus den gesammelten Informationen leitet CLEARER eine Compliance-Entscheidung ab und setzt diese mit Hilfe von macmon NAC im Unternehmensnetzwerk durch. So setzt CLEARER für ein Endgerät, das nicht den Unternehmensrichtlinien entspricht den Compliance-Status „noncompliant“, was über eine voreingestellte Regel für die Isolation eines Endgeräts sorgt, indem es ins Remediation-VLAN verschoben oder der Netzwerkanschluss am Switch abgeschaltet wird. Die Web-GUI von macmon enthält im Compliance-Bericht einen ausführlichen Überblick darüber, aus welchen Gründen die jeweiligen Endgeräte isoliert wurden. In der SIEM-GUI von CLEARER kann hingegen der Vorfall im Detail und eine Handlungsempfehlung nachgelesen werden.

Übertragung der Endgeräte

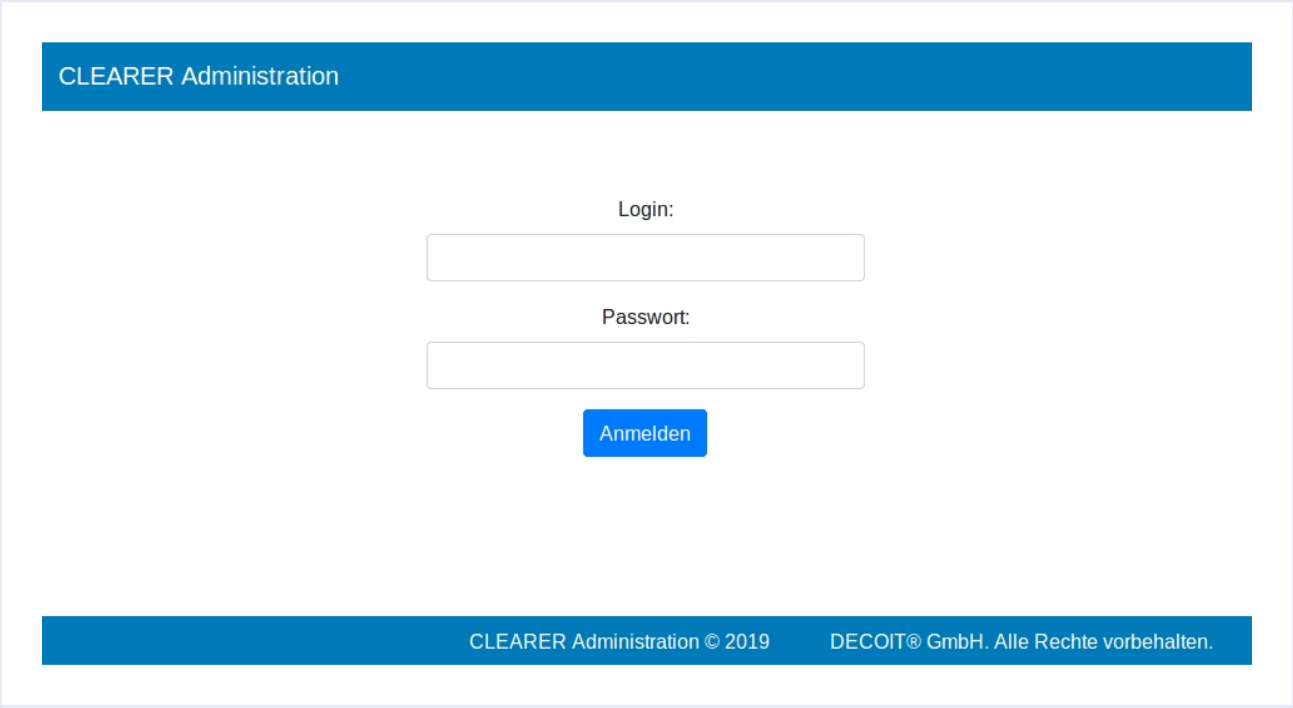
CLEARER sammelt Informationen über Endgeräte im Unternehmensnetzwerk. In regelmäßigen Intervallen fragt es dabei auch den Datenbestand der Endgeräte von macmon NAC ab und vervollständigt damit die eigene Übersicht über alle Endgeräte, um einen optimalen Schutz zu bieten. Denn bei den erkannten Vorfällen muss CLEARER zwischen bekannten und unbekannten Endgeräten unterscheiden, um Anomalien sicher erkennen zu können. Über die SIEM-GUI kann auf einen Blick dabei immer das Sicherheitsrisiko des Unternehmens erkannt werden bzw. ob der zuständige IT-Administrator eingreifen sollte.

Konfiguration von CLEARER

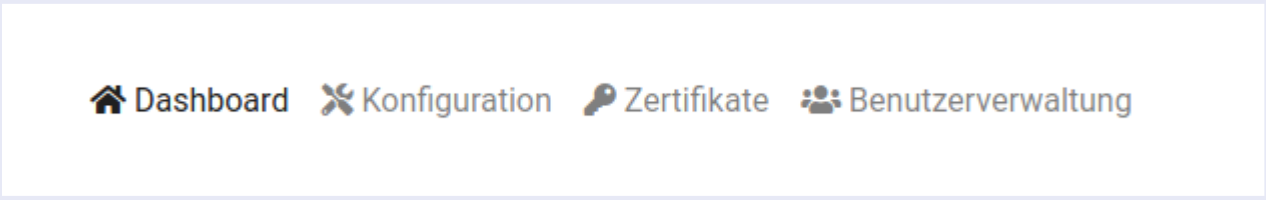
Die Installation und Konfiguration von CLEARER ist in der Anwendungsdokumentation enthalten, die bei Auslieferung mitgeliefert wird. Diese besteht aus der Software-Installation, -Einrichtung und der Funktionsbeschreibung.

Die Konfigurationsschritte, die spezifisch macmon betreffen, werden hier noch einmal herausgestellt:

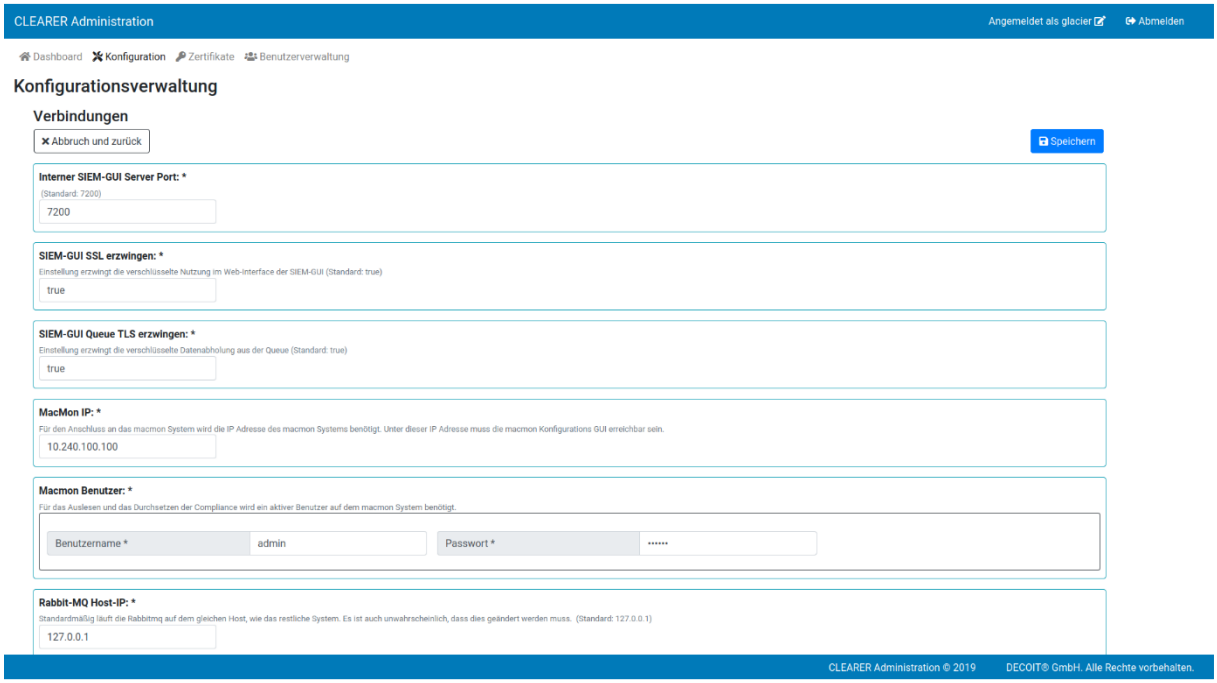
1. Nach Aufruf der CLEARER Management-Oberfläche, können Sie sich mit dem Benutzernamen root und dem zuvor generierten Passwort anmelden.



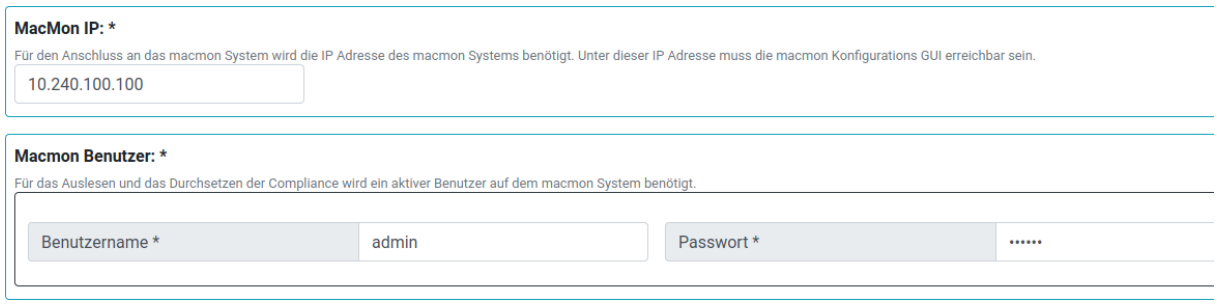
2. Die Konfiguration für die Komponenten kann über den oberen Reiter erreicht werden. Die Konfiguration ist in sechs Kategorien gegliedert. Die Kategorien entsprechen dabei nicht den einzelnen Komponenten, sondern sind inhaltlich gegliedert. Um eine Komponente zu konfigurieren sind also gegebenenfalls Änderungen in mehreren Kategorien notwendig. Klicken Sie auf Konfiguration.



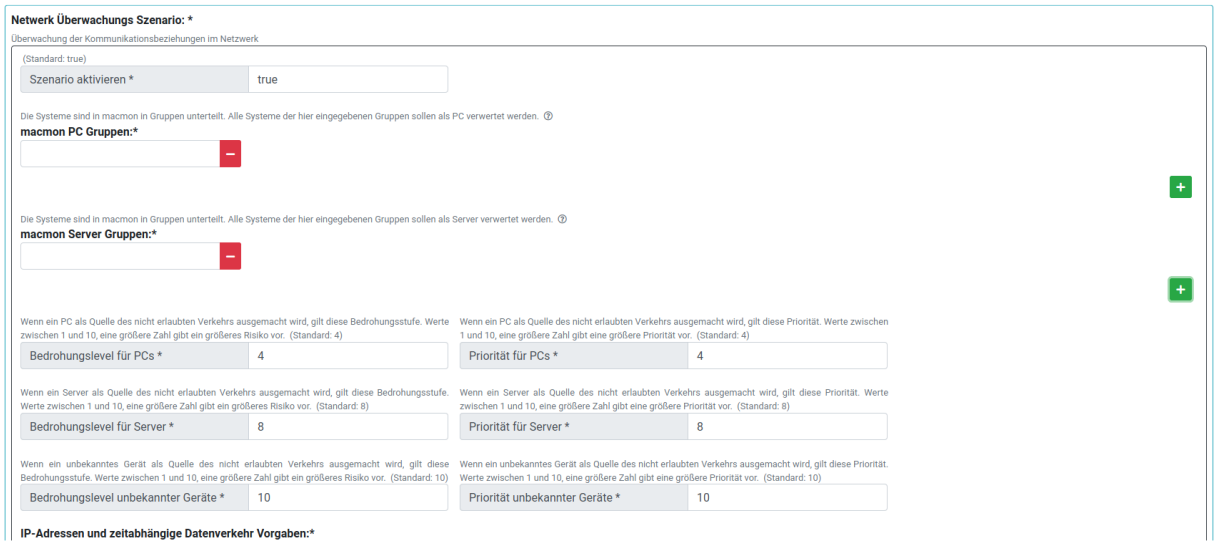
3. Klicken Sie danach auf die Kachel Verbindungen. In der Verbindungen-Kategorie finden sich die Konfigurationen für die Verbindungen



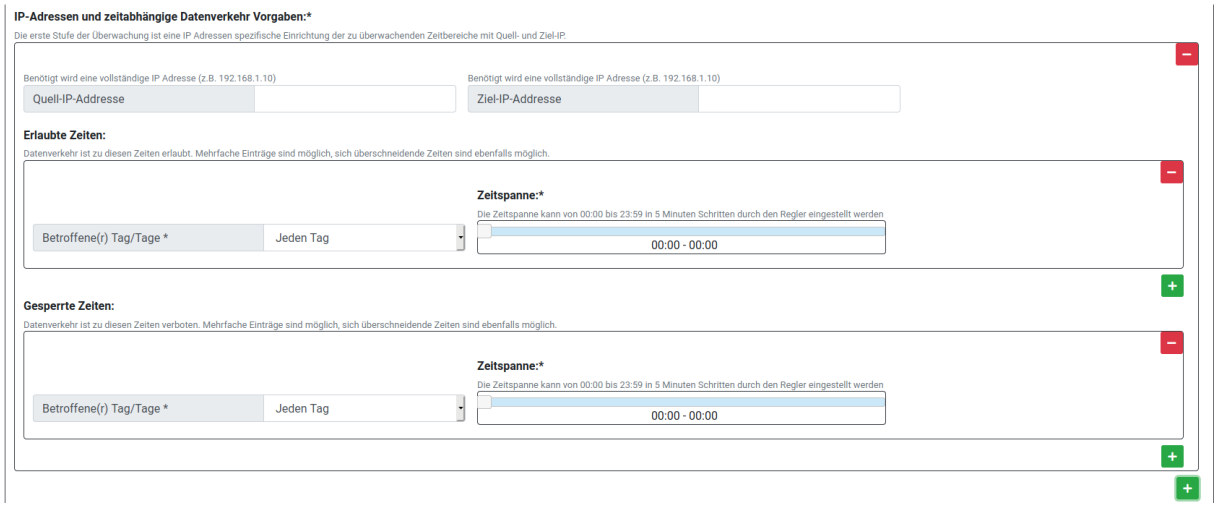
4. Hier können die Anmeldedaten für die macmon-Instanz hinterlegt werden. Fehlen diese Daten dann können IP-Adressen nicht zu MAC-Adressen aufgelöst werden und es ist nicht möglich direkt aus der SIEM-GUI Maßnahmen zu ergreifen.



5. In der Szenarien-Kategorie können die Parameter und Regeln für die beiden aktiven Szenarien definiert werden. Hier kann außerdem definiert werden, welche Netzwerke *Zeek* überwachen soll und an welchem Netzwerkinterface gelauscht werden soll. Ein Vorfall für eine Regelverletzung wird nur erstellt, wenn sich die IP-Adresse oder das Netzwerk in den für *Zeek* zur Überwachung festgelegten Bereichen befindet, sonst werden die Informationen bereits bei *Zeek* verworfen und erreichen nie die Analysekomponente.



6. Hier kann eine Unterscheidung von Workstations uns Servern mittels eigener Macmon-Gruppen vorgenommen werden, außerdem lassen sich hier individuelle Bedrohungslevel festlegen um später eine bessere Einschätzung des Risikos zu ermöglichen.



7. Schließen Sie die Konfiguration ab.

Konfiguration von macmon NAC

Es muss macmon NAC nicht separat konfiguriert werden. Der Austausch zwischen beiden Systemen geschieht über die Rest-API- oder macutil-Schnittstelle. Dafür wurde ein NAC-Actuator in CLEARER integriert.

Kontakt bei der DECOIT® GmbH

Prof. Dr. Kai-Oliver Detken (Vertrieb)
E-Mail: detken@decoit.de
Tel.: 0421-596064-0
Fax: 0421-596064-09

Timo Klecker (Entwicklung)
E-Mail: klecker@decoit.de
Tel.: 0421-596064-0
Fax: 0421-596064-09

Henrik Gießel (Technik)
E-Mail: giessel@decoit.de
Tel.: 0421-596064-0
Fax: 0421-596064-09

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu