



MACMON NAC WHITEPAPER

Anbindung an FireEye Network Security

Inhaltsverzeichnis

Einleitung	3
Anwendungsfälle	3
FireEye Network Security übermittelt Informationen an macmon NAC.....	3
Konfiguration von macmon NAC.....	4
Konfiguration der FireEye Network Security-Integration.....	4
Konfiguration von FireEye Network Security.....	5
Benachrichtungen	5
Hinzufügen eines HTTP-Servers	5
Konfiguration der Verbindung.....	6
Kontakt bei FireEye.....	6

Einleitung

FireEye Network Security ist eine effektive Cybersicherheitslösung, die komplexe, gezielte und im Internetverkehr versteckte Angriffe in Echtzeit aufdeckt und abwehrt und damit das Risiko kostspieliger Sicherheitsverletzungen senkt. Zudem liefert FireEye Network Security binnen weniger Minuten konkrete Beweise, verwertbare Daten und Handlungsempfehlungen für die effektive Behebung der aufgedeckten Sicherheitsvorfälle. Mit FireEye Network Security können sich Unternehmen effektiv vor Bedrohungen schützen – unabhängig davon, ob diese eine Schwachstelle in Windows, macOS oder einer bestimmten Anwendung ausnutzen, ob der Hauptsitz oder eine Niederlassung angegriffen wird und wie gut die Bedrohung in dem umfangreichen eingehenden Internetdatenverkehr versteckt ist, der in Echtzeit überwacht werden muss.

Anwendungsfälle

FireEye Network Security übermittelt Informationen an macmon NAC

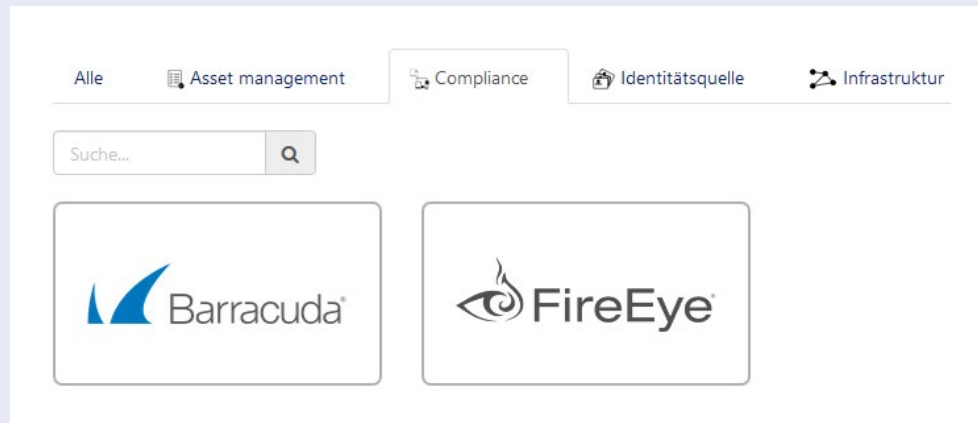
Ransomware kann das Leben eines Administrators hart machen. Wenn eine Ransomware trotz aller Vorsichtsmaßnahmen ein Endgerät infiziert, geht es bei der Isolierung dieses Endgeräts aus dem Netzwerksegment um Sekunden. Dadurch wird verhindert, dass sich eine Schadsoftware über das Netzwerk verbreitet und andere im Netzwerk befindlichen Ressourcen verschlüsselt. Mit seiner fortschrittlichen Engine zur Erkennung von persistenten Bedrohungen ist FireEye Network Security in der Lage, eine Bedrohung im Unternehmensnetzwerk im Handumdrehen zu erkennen. Der Zusammenschluss aus FireEye Network Security und macmon NAC ist eine leistungsstarke Kombination aus Erkennung von Bedrohungen und Isolation von betroffenen Endgeräten.

macmon NAC ermöglicht es FireEye Network Security, den Compliance-Status eines Endgeräts basierend auf dem von FireEye Network Security festgestellten Systemstatus zu erzwingen. Dies gilt für Netzwerke jeglicher Größe, denn in jedem Netzwerk finden Sie Geräte, die möglicherweise Bedrohungen ausgesetzt sind. Wenn FireEye Network Security eine solche in Ihrem Netzwerk erkennt, klassifiziert es die gefundene Malware. Anschließend schickt es eine Benachrichtigung an die Compliance-Schnittstelle von macmon NAC, die Informationen über die IP-Adresse und den Namen der identifizierten Malware enthält. macmon NAC verarbeitet die Informationen und setzt den Compliance-Status des infizierten Endgeräts auf „non-compliant“. Eine voreingestellte Regel isoliert dann dieses Endgerät, indem es ins Remediation-VLAN verschoben oder der Netzwerkanschluss am Switch abgeschaltet wird.

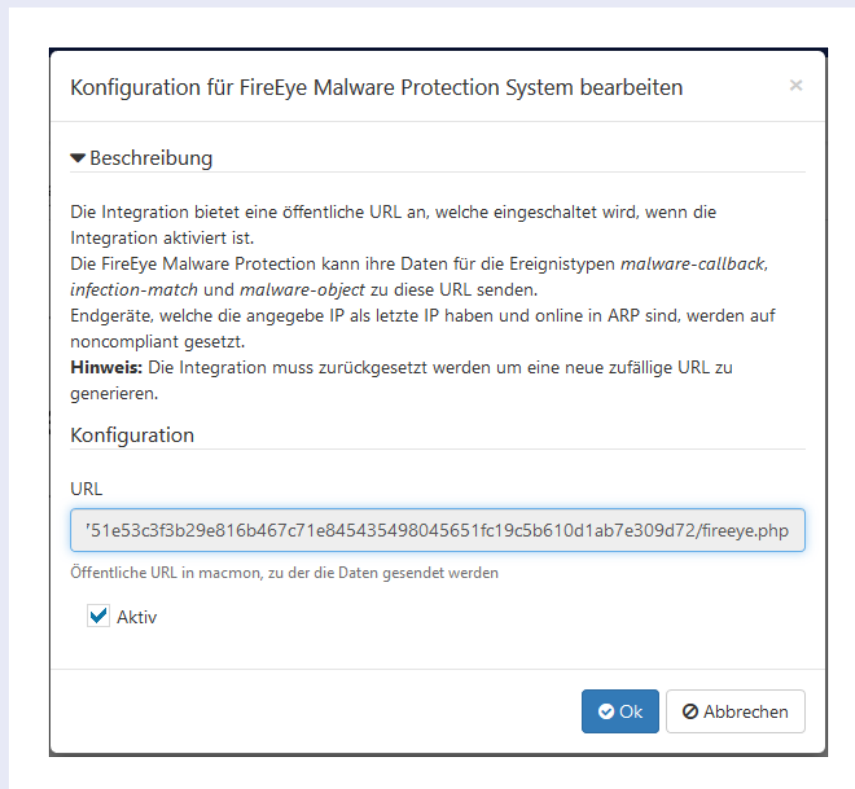
Konfiguration von macmon NAC

Konfiguration der FireEye Network Security-Integration

Die Konfiguration wird über das Web-GUI durchgeführt. Tippen Sie auf Einstellungen und Drittanbieter-Integrationen, dann auf Compliance.



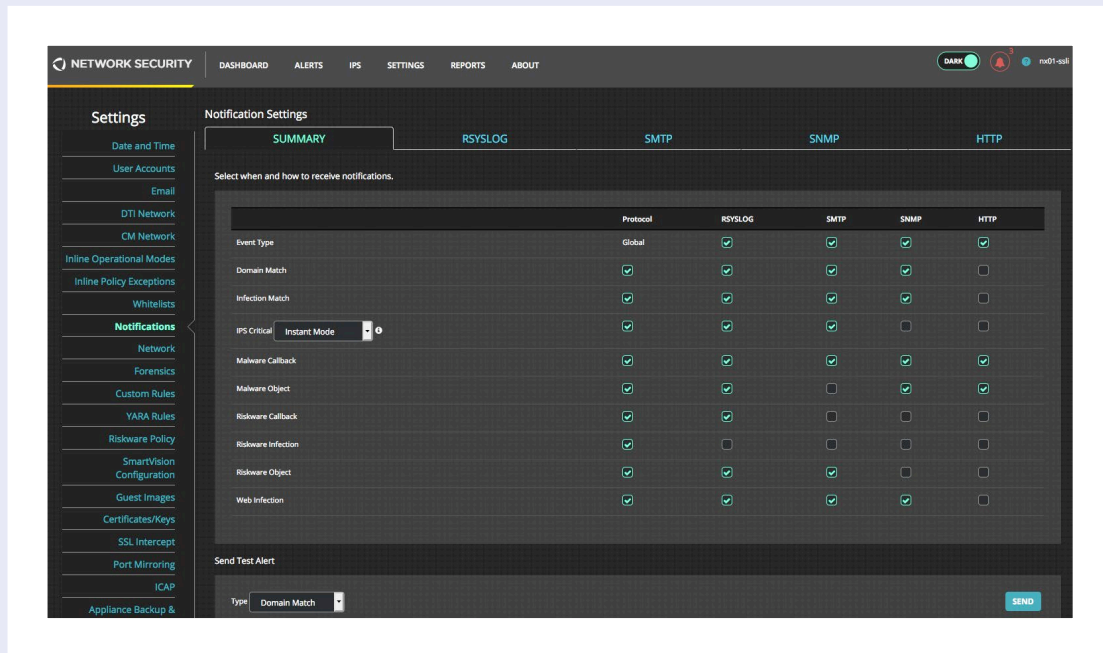
Wenn der Rahmen der FireEye-Kachel grau ist, ist die Integration noch nicht aktiviert. Bitte tippen Sie auf die Kachel, um den Konfigurationsdialog aufzurufen. Kopieren Sie anschließend die für Sie generierte URL aus dem Konfigurationsdialog in die Zwischenablage, da Sie diese zur Konfiguration von FireEye Network Security in dessen GUI benötigen werden. Bitte setzen Sie den Haken bei *Aktiv* und tippen Sie auf „Ok“, um die Integration zu aktivieren.



Konfiguration von FireEye Network Security

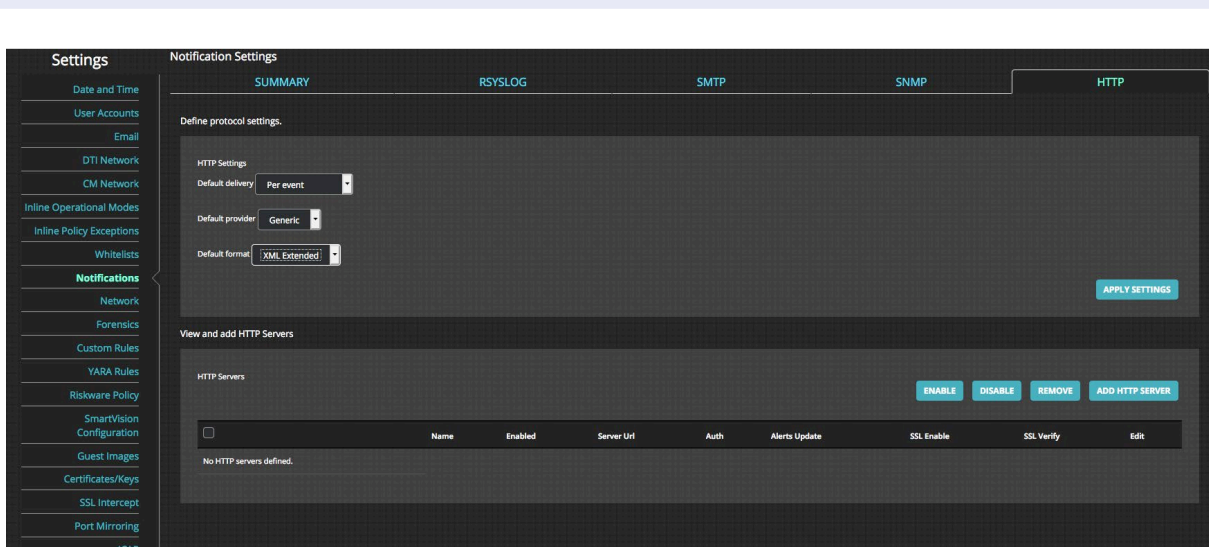
Benachrichtigungen

1. Tippen Sie auf Settings in der oberen Navigationsleiste.
2. Tippen Sie auf Notifications in der linken Navigationsleiste.
3. Setzen Sie die Haken in der Spalte HTTP für „Malware Callback“ und „Malware Object“.



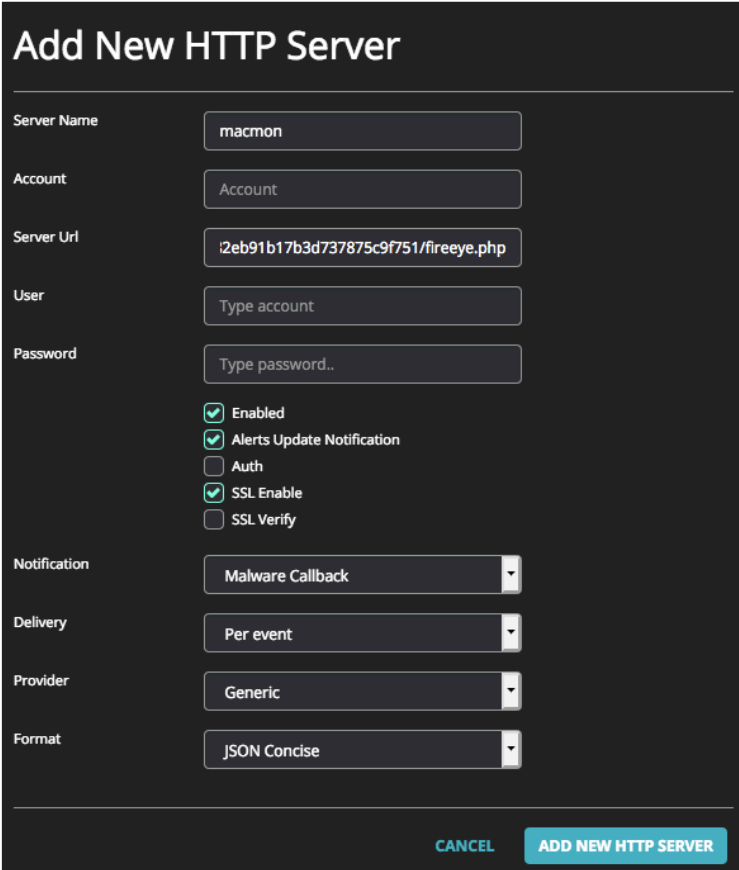
Hinzufügen eines HTTP-Servers

1. Tippen Sie auf das HTTP-Tab, das Sie im Screenshot sehen können.
2. Tippen Sie auf ADD HTTP SERVER im Bereich View and add HTTP Servers.



Konfiguration der Verbindung

1. Geben Sie einen Servernamen ein, der Ihrer Konfiguration am besten entspricht.
2. Fügen Sie die zuvor kopierte URL als Server Url ein.
3. Setzen Sie die Haken bei Enabled, Alerts Update Notification, SSL Enable. Setzen Sie SSL Verify nur, wenn Sie ein offiziell signiertes SSL-Zertifikat einsetzen.
4. Wählen Sie „Malware Callback“ bei Notification.
5. Wählen Sie „Per event“ bei Delivery.
6. Wählen Sie „Generic“ bei Provider.
7. Wählen Sie „JSON Concise“ bei Format.



The screenshot shows a dark-themed configuration form titled "Add New HTTP Server". The form contains the following fields and options:

- Server Name:** Input field containing "macmon".
- Account:** Input field containing "Account".
- Server Url:** Input field containing "i2eb91b17b3d737875c9f751/fireeye.php".
- User:** Input field containing "Type account".
- Password:** Input field containing "Type password..".
- Checkboxes:**
 - Enabled
 - Alerts Update Notification
 - Auth
 - SSL Enable
 - SSL Verify
- Notification:** Dropdown menu with "Malware Callback" selected.
- Delivery:** Dropdown menu with "Per event" selected.
- Provider:** Dropdown menu with "Generic" selected.
- Format:** Dropdown menu with "JSON Concise" selected.

At the bottom right, there are two buttons: "CANCEL" and "ADD NEW HTTP SERVER".

Kontakt bei FireEye

Wenn Sie Fragen haben, kontaktieren Sie FireEye bitte unter <https://www.fireeye.com/support/contacts.html>

Kontakt

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