PRESS RELEASE

Integration between macmon NAC and Greenbone Security Manager now available

Berlin, 08.02.2021: Greenbone Security Manager (GSM) from Greenbone Networks identifies **security gaps in a company's IT systems** and evaluates their potential risk. In addition, GSM recommends actions to resolve any detected vulnerabilities.

The aim is to identify possible points of attack from cyber criminals and to prevent these attacks. Experience has shown that in 999 out of 1,000 cases, companies had already been aware of the vulnerabilities exploited by attackers for at least 12 months. This solution includes a **daily security update**, which checks for over 87,000 network vulnerabilities. The turnkey appliance solution is based on Open Source software and takes just 10 minutes to run. The private company, based in Osnabrück, Germany, was founded in 2008 by leading experts in the fields of network security and Open Source software. Greenbone Networks has been a technology partner of macmon secure GmbH since 2018.

macmon NAC ensures that any new endpoints are scanned for malware by Greenbone Security Manager when they are added to the corporate network and regularly evaluates the **compliance status** in order to protect the network.

***Christian Bücker, Managing Director of macmon secure GmbH**, reports:*
"It is vital that a corporate network bescanned regularly to maintain IT security. The result of this scan is provided by GSM and evaluated at regular intervals by macmon NAC. If the device complies with company policies, it will be permitted to access the corporate network. If the device does not comply with the policies, macmon NAC can isolate the endpoint by means of a configurable response or disconnect it from the network and notify the administrator. This ensures that network access control is fully compliant at all times."

macmon NAC recognizes new and known endpoints and initiates scans

New devices are constantly being added to a corporate network. An administrator usually ensures that a new device is not infected with malicious code and does not pose a threat to data integrity or network security. macmon NAC detects a new endpoint when it is connected to the network and orders GSM to perform a scan. Depending on the result of this scan, access is either granted or denied.

macmon NAC also detects a known endpoint and initiates a scan by GSM if the device has been disconnected from the network for too long. Some endpoints cannot be scanned regularly because they are not permanently connected to the corporate network. For example, an employee in the field can be away from home for days or weeks. When the employee returns home, the endpoint reconnects to the corporate network, macmon NAC detects the device and instructs GSM to perform a scan. The result of this scan is provided by GSM: If the device complies with company policies, it will be permitted to access the corporate network. In the same way as a new endpoint, if the known device does not comply with the policies, macmon NAC can isolate the endpoint by means of a configurable

response and notify the administrator. macmon NAC thus regularly **checks the integrity of new and temporarily disconnected endpoints**, according to the time period specified by the user.

As **Christian Bücker, Managing Director of macmon secure GmbH,** explains: *"The great advantage of this integration is that as soon as macmon NAC detects the presence of an endpoint, a scan is carried out immediately and fully automatically. If the device is not compliant, macmon NAC is informed directly and responds immediately and automatically with a device lockout or quarantine. The key to success is fast,* ***automatic responses without the need for administrator intervention****. By combining the strengths of the two solutions, the* ***security concept will naturally be enhanced****. macmon NAC is able to detect new devices added to the network very quickly and enforce security rules on behalf of Greenbone where it is not able to enforce these rules itself. Greenbone, on the other hand, is highly adept at identifying vulnerabilities, which is not macmon's area of expertise."*

Greenbone Security Manager is easy to integrate via the web GUI: Whitepaper Greenbone

About macmon secure GmbH:
macmon secure GmbH — the German technological leader for network access control
The experienced IT experts have been offering manufacturer-independent, BSI-certified solutions since 2003. These solutions protect heterogeneous networks from unauthorized access through immediate network transparency. macmon is quick and easy to implement and offers considerable added value for network security. macmon can be integrated with other security solutions from international technology partners, such as endpoint security or firewall. Customers obtain an immediate network overview with graphical reports and topology. In addition, macmon offers customers and partners an extensive training program and 24/7 support from Germany. This makes macmon a key IT component in the areas of digitization, BYOD or intent-based networking.

For further information, visit: www.macmon.eu
Twitter: https://twitter.com/macmon_EN
YouTube: www.youtube.com/user/macmonsecure
LinkedIn: https://de.linkedin.com/company/macmon-secure-gmbh

Contact Person at macmon secure GmbH:
Christian Bücker | CEO
macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin
+49 30 2325777-0 | nac@macmon.eu | www.macmon.eu