SEPIO Solutions backed by Munich Re Group

CASE STUDY

SEPIO SYSTEMS

Munich RE

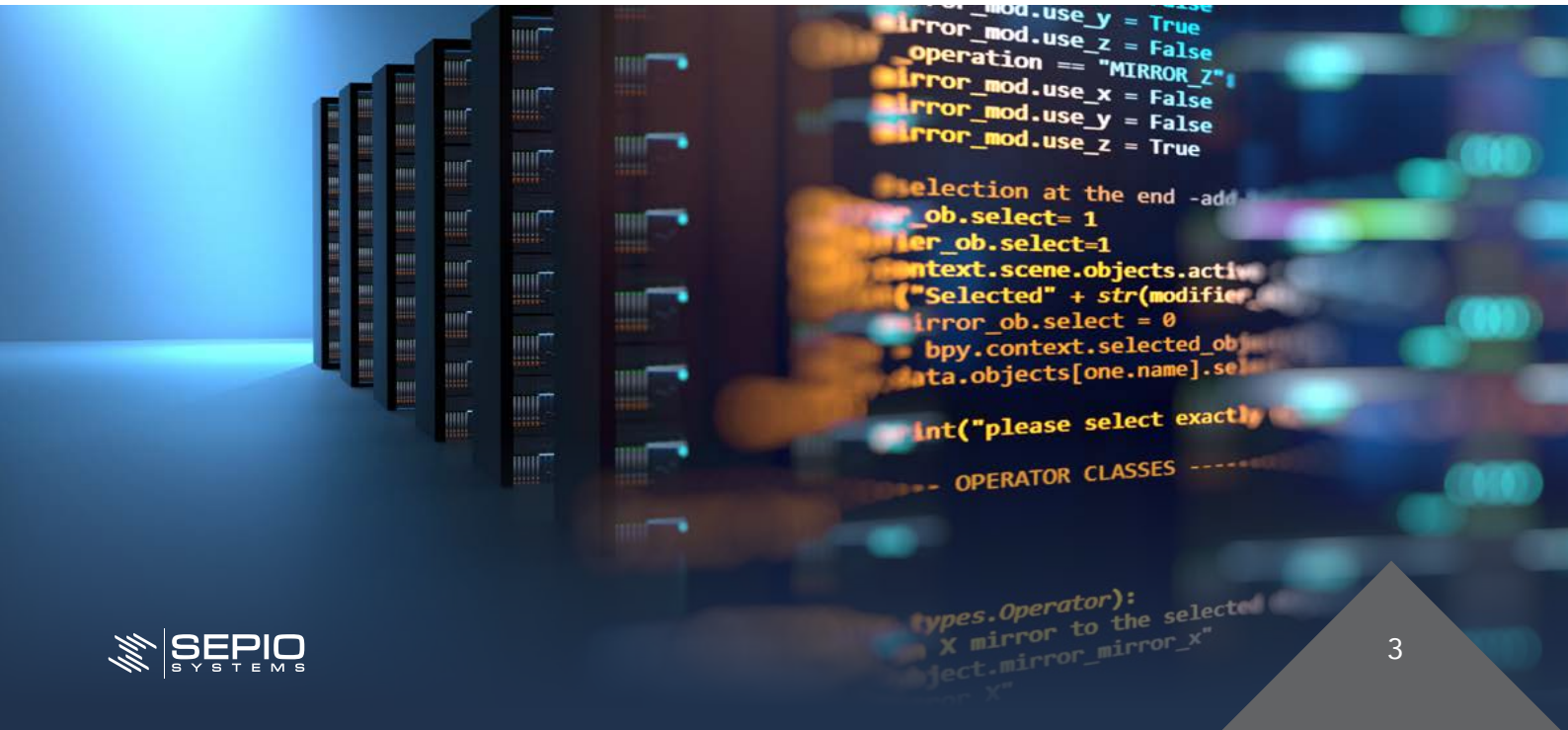
"THE NETWORK VISIBILITY CREATED BY SEPIO'S SOLUTION IS A CRITICAL COMPONENT OF ANY EFFECTIVE ROGUE DEVICE MANAGEMENT SOLUTION."

Frost & Sullivan

The Rogue Hardware Problem

Cyber Crime organizations and state sponsored groups use manipulated hardware or firmware, delivered directly by humans or through the supply chain, to carry out their attacks. Existing Cyber Security products lack the required level of visibility that is crucial to mitigate these types of risks. The attackers are very much aware of these limitations and, in recent years, focus on this attack vector.

Multiple incidents were revealed, yet most of them didn't go public. Those which did, for example the NASA JPL Raspberry Pi incident, shed some light on how these attackers are using Physical layer attack tools to hack into highly secured IT/OT infrastructure assets.



Sepio's Solution to the Rogue Hardware Problem

Sepio Systems' software-only solution provides complete visibility to whatever is connected over the client's entire Enterprise; whether it be connected directly to an Endpoint or as concealed as a Network element.

Sepio's solution provides visibility starting from the Physical layer, making sure that no device goes undetected. Its unique detection algorithm provides the much-needed mitigation from Rogue Devices, even when they perfectly impersonate legitimate devices that were previously approved by other security solutions.

A company no longer needs to rely on the specific discovery or management features of devices in order to detect and block them when they are rogue. Sepio Systems delivers a simple solution that requires very few resources, providing immediate value to the client.

Sepio Systems' solution connects to the existing infrastructure, extracts all the physical layer information, analyzes it using a novel algorithm – which is based on physical finger printing and enhanced by a Machine Learning

module – and provides an extensive report with clear, actionable measures.

The software is augmented by real-time cloud-based intelligence that provides early warning of the latest malicious hardware and threat patterns.

The SaaS-based security suite can be deployed on any physical or virtual environment in any combination of on-premises, private and public cloud. With its "read-only" privileges, SepioPrime, which orchestrates Sepio's solution, cannot change or alter anything within the organization. By suppling organizations with full visibility of the enterprise's IT assets, a stronger cybersecurity posture is achieved.

Sepio Systems' team, directors and advisors is made up of experts from the industry, CIA, Mossad and the Israeli NSA. The complete detection capabilities of Sepio's solution comes from utilizing their years of experience in cyber operations and supply chain and hardware manipulations.Sepio's software-based Physical layer security solution is unique in the market.

SEPIO Solutions backed by Munich Re Group

Sepio Systems' solution is now offered with a performance guarantee insured by Munich Re Group. Thus, Sepio's customers are now even better protected. They will not only have coverage of the physical layer, but also an additional financial safety net in case the security software would actually fail to safeguard the client.

Based on a thorough assessment, Munich Re put capital behind the risk of Sepio's solution not performing as promised. Hence, providing a strong indication of the efficacy of Sepio's security solution. This favorable signal saves testing efforts on the part of the AI client, including search and analysis costs.

Additionally, the trust which Munich Re puts into Sepio's solution makes it easier for an organization's decision makers to purchase the software as there is significantly less uncertainty. Based on that, Sepio's clients can grow without being perturbed by the threat of potential hardware attacks.

Munich Re's offering for artificial intelligence companies

As buyers of AI software delegate significant responsibilities to the software, they face the crucial question whether the model will perform as promised. In order to alleviate such doubts Munich Re offers risk transfer solutions, like the one for Sepio, for a broad range of AI software providers.

The balance sheet, brand, and technical expertise of Munich Re provide a signal of trust, safety and credibility for the AI user. This trust complements the AI service and creates a unique selling proposition for the AI provider. So Munich Re can help to accelerate its partners' sales, new market access, growth rates and investor attractiveness.

Performance promises are transformed into financial commitments – creating peace of mind.

Sepio contact - How to Lower Your Risk

Visit us at **www.sepio.systems** to find out more about our solution and the risks of Rogue Devices. Here, you can contact our sales team to discuss how Sepio Systems can protect your organization. Even better, we provide demos to give a visual representation of how our solution works once deployed. Please do not hesitate to reach out to us with any questions or inquiries.

We are also available on:

Linkedin >>

https://www.linkedin.com/company/sepio-systems/

Facebook >>

https://www.facebook.com/cybersepiosystems/

Twitter >>

https://twitter.com/sepiosys

<< LEARN MORE >>

SEPIO SYSTEMS