SECURITY CHECKUP

Ever heard of Zero Day attacks, Trojans, Worms, Bots, ...
Your corporate network offers access to valuable and sensitive information, but is always open to fall into hands of those security threats.

Are you sure there aren't any hidden "surprises" threatening your corporate network from all over the world ? Do you know that in 75% of the organizations bots are found ? Do you know that in 75% of organizations P2P file sharing were detected in use by employees ?
Do you know that in 33% with at least one unknown form of malware ?
According to these organizations are still vulnerable to every day security threats ?

INIA provides you with a Security Checkup to provide you with an security status overview of your corporate network!

During the Security Checkup assessment an INIA Consultant deploys a Check Point security gateway within your network, inspecting traffic traversing the existing firewall. It inspects the traffic using a mirror port on a network switch. A mirror port doesn't transmit any traffic onto your existing network, eliminating the risk of downtime or major changes to the existing network configuration.

The INIA Consultant sets up the Security Gateway by enabling all the necessary security features, which might include Application Control, URL Filtering, Data Loss Prevention, IPS, Anti-Bot, Anti-Virus, ...
The Security Gateway will then be connected to the mirror port in order to start capturing the network traffic.
The Security Gateway will remain in place for at least a week to allow thorough inspection. The longer the time period of analysis, the better.

After removing the device from the network the INIA Consultant will analyze the results and generate the Security Checkup report. The report covers a full range of security risk in detail:

- High risk web applications and websites used by employees such as: P2P File Sharing applications, Proxy anonymizers, File Storage applications, malicious websites and more
- Analysis of malware threats including computers infected with bots, viruses, and unknown malware (zero day attacks and malware that cannot be detected by traditional anti-virus systems)
- Exploited vulnerabilities of servers and computers in the organization, indicating possible attacks
- Sensitive data sent outside the organization via emails or the web
- Bandwidth analysis identifying the top bandwidth consuming applications and accessed websites to understand who and what is hogging your network bandwidth

The INIA Consultant will provide you with a detailed threat analysis report and will go over this report with you, which includes all security incidents detected during the assessment and the recommendations on how to protect against these threats.

To schedule a Security Checkup please contact your account manager or

Presales Division Inia
T +32 3 545 67 89
security.checkup@inia.be

inia Check Point SOFTWARE TECHNOLOGIES LTD. Xylos