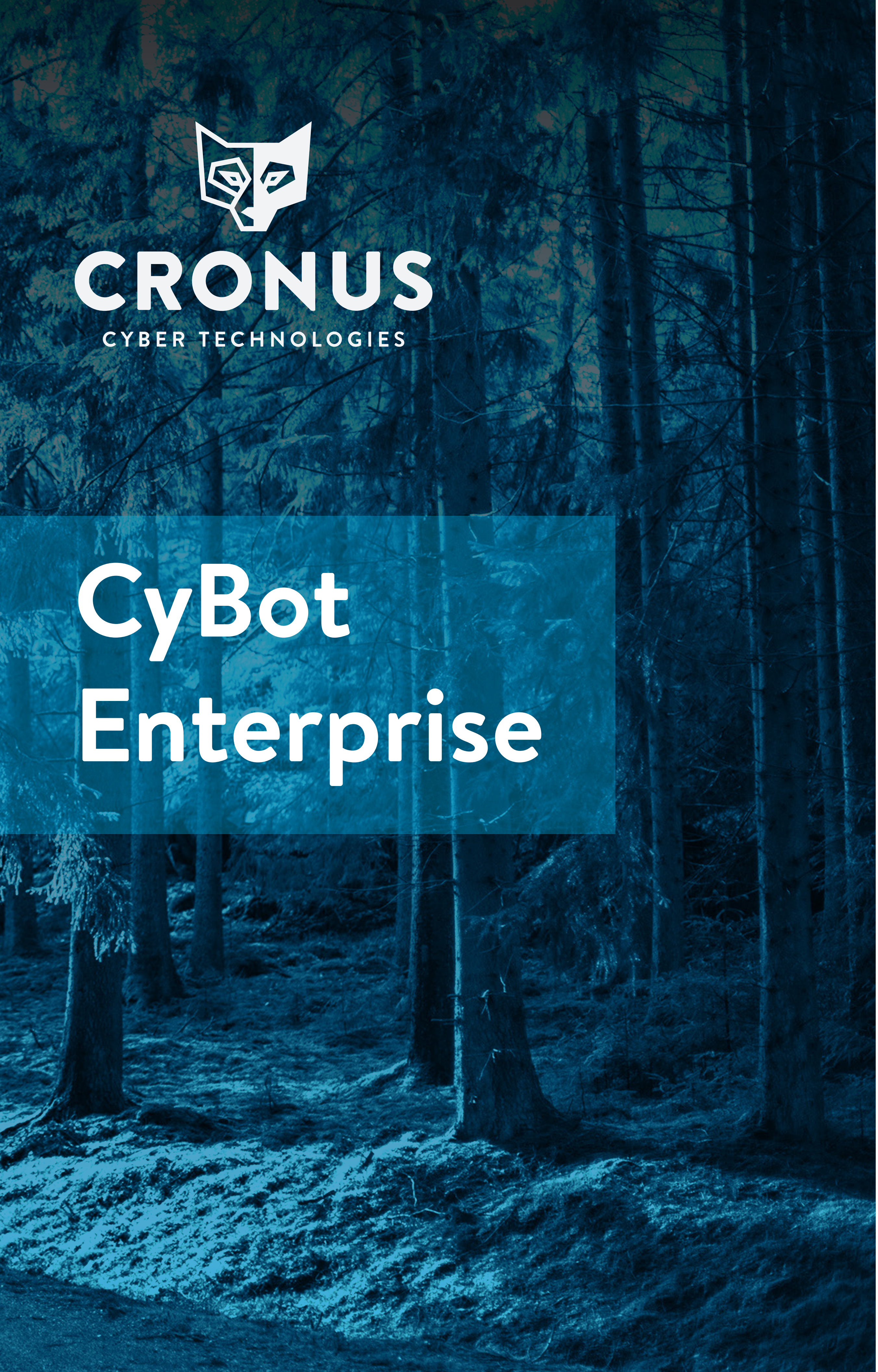

CRONUS

CYBER TECHNOLOGIES

CyBot Enterprise

Overview

In the industry today, hackers are becoming more and more sophisticated and knowledgeable, and the threats are multiplying periodically globally, so organizations are substantially increasing their security budget. At the same time CISOs are disappointed that they cannot actually assess their risks and the directions from which a successful hacking attack can materialize. **As the organizations are becoming more and more complex and dynamic there are so many ways for a hacker to be successful. Today, CISO's feel a bit at limbo and are never sure how secure their systems and environment really is.**

It's time to change this point of view. With multiple copies of CyBot Pro you really have hundreds of white hackers that work in your organization, 24/7, trying to find your vulnerabilities and how your systems may be exploited.

Their finding are then display in an aggregate way on the CyBot Enterprise Dashboard. In addition CyBot Enterprise allows the different CyBot Pro's to interact building multi domain / site attack scenarios, identify patterns of vulnerabilities and present them on one unified Dash board.

This capability allows the security team, for the first time, to plan the security system in the way that corresponds to the specific needs and threats identified by CyBot Enterprise global view. Repeating the pen testing every few hours, allows for analyzing and fixing vulnerabilities by location, criticality and frequency. For example:

- Address range, from which the hacking attacks can come – e.g., the network switches, a specific branch, or from specific system like: VoIP, ERP, etc.
- Controlling – why – e.g., the system provides information about critical vulnerabilities, that have not been dealt with, as yet.

Once the system has found the locations from which possible attack scenarios can originate, it is easier to properly consider how to deal with the threat and mitigate it? For example:

- If most attack scenarios are derived from the ability to connect a variety of devices that do not share the same security requirements, then it may be correct to invest by connecting them to the NAC or upgrading the NAC.
- If there are many dangerous attack scenarios, which are based on WEB interfaces, the solution should be to harden the access to these interfaces and the database connectivity interfaces.

CyBot Enterprise

Now with CyBot Enterprise, as the Information Security manager, you can achieve a number of important overall advantages:

- Ability to purchase security systems, based on relevant threats to the organization, and thus improve your decision processes based on CyBot Enterprise dashboard and reports.

- Provide sophisticated security solutions, because the system can detect failures, which cannot be detected from a single scan (e.g., multi domain / location attack scenarios).

- Ability to identify patterns of attack scenarios and respond to them accurately and in a timely manner.

CyBot Enterprise, locates and aggregates the vulnerabilities from the distributed CyBot Pros and thus prevents the action of penetration and leakage of information, since the defects are detected and treated in advance.

The CyBot Enterprise version provide a centralized management interface for all systems installed in the organization (for definition, monitoring and results viewing and analysis). This management interface allows some major capabilities such as:

- The ability to update data into the CyBOt Pros from a central management station.

- The system will create global attack scenarios, for example: finding vulnerabilities in routers spread across the organization in different countries, and test the integrated dangerous global scenarios and reports results.

- A global perspective on vulnerabilities across the enterprise (aggregated from multiple CyBot Pros). The main console Collects information from all CyBot Pro machines that are located in all branches and departments, and represent the results in a global risk mitigation view.

- CyBot Enterprise can be easily interfaced with command stations (e.g., NAC). It can immediately send commands to security systems e.g., instruct the NAC to block connections that enable a critical scenario on all relevant network components. In this way, the hacker will not find any possibility to attack via the specific vulnerabilities closed by this scenario.

- Precise estimates and actions require clear cut information about every critical vulnerability, at every level within the enterprise; good valuation on the importance of all assets and business activities. The user can instruct CyBot Enterprise on what are the critical assets and resources. This information will be used by the CyBot integrated solution to build additional attack scenarios for these specific resources hardening their resistance to hacking attacks. In this way, you will be able to build a relevant risk map for your organization, and define the most suitable security design for these critical assets and resources.