proximus NXT

Cybersecurity

Orbit Managed XDR

Date 01/01/2024

Why Detection and Response is essential in increasing your organizations Cybersecurity maturity

In today's inherently hostile environment, even the best designed security environment, equipped with the most modern and up-to-date firewalls and other protection measures, cannot be called 100% secure. Indeed, today, cyber-attacks have become so smart that it is impossible to stop all attacks. Hackers use artificial intelligence and machine learning to bypass layers of protection and lure your customers employees into their trap.

Protection and prevention alone are no longer enough - an organisation should also arm itself and prepare itself to detect breaches and take quick action when hackers have managed to find their way into the systems and data of the organization. It is very important to continuously monitor business systems, company data and the identities of employees and identify suspicious anomalies as soon as possible. And of course, to take immediate action if a suspicious situation turns out to be a cyber-attack, to mitigate any potential impact to the maximum extent possible.

The main reasons for organizations to implement detection and response are:

- Information protection. Data is everywhere nowadays, in the cloud, on mobile devices, in SaaS applications like Office 365, et cetera. When data is lost, it can damage the reputation of an organisation, put intellectual property in the hands of competition, remove trust from the customers or even lead to GDPR fines. Detection and response are required to keep track of where all the data is and to detect and stop data leakage as soon as possible.
- Compliancy. There is an ever-increasing pressure to improve the cyber security maturity of organizations. Regulation and standards like NIS2, DORA, GDPR, ISO27001, et cetera, prescribe that detection and response is implemented and that an organization is able to report breaches to authorities in a short time frame (e.g. 72 hours). And today it is impossible to get a cybersecurity insurance without detection and response in place.
- Resilience. Business and production disruption is the worst nightmare for many organizations, especially for hospitals and industrial companies. And cyberattacks like ransomware attacks are notorious for their ability to take down businesses. Many organizations therefor focus on resilience; the ability to keep the business running, not matter what happens. Detection and response plays a crucial role in cyber resilience, as a fast detection and imminent response will reduce the impact and potential downtime to a minimum.=

proximus NXT

How eXtended Detection and Response (XDR) solutions are used for Detection and Response

For many years, the analysis of security incidents was only possible with a Security Information and Event Management (SIEM) solution. Such a solution correlates security logs from different systems from different vendors and searches for "indicators of compromise" using predefined use cases, which trigger the creation of a notable event or alert.

In recent years, more and more security vendors have started offering "Cross/eXtended Detection and Response" or XDR solutions that perform log correlation across their different solutions, without the need for a SIEM. Microsoft Defender is a prominent example of such a XDR solution. These XDR solutions provide ready-to-be-analyzed alerts, as the vendor takes care of the correlation of the logs. The security vendors create the use cases as part of their XDR offering and they also apply Artificial Intelligence and Machine Learning to automate use case creation and refinement. This greatly reduces the maintenance costs and at the same time improves the quality of the log correlation. XDR solutions also offer many off-the-shelf response actions that use the protection capabilities of the solutions of the XDR vendor to contain and remove threats. Examples of response actions are endpoint isolation, user account lock, URL blacklisting, et cetera.

At the same time there is a trend at many organizations to reduce the number of security vendors and to consolidate their security architecture. This trend reduces the need for multi-vendor log correlation. As a result, these new XDR solutions become an interesting alternative for a SIEM solution.

Orbit Managed XDR unburdens your organization by taking care of its XDR security alerts 24/7

The Proximus Orbit Managed XDR service manages the alerts generated by the XDR solution of your organization. Proximus currently supports Microsoft Defender, Palo Alto Cortex XDR, and Fortinet FortiAnalyzer as XDR platforms. The Proximus SOC analyses these alerts 24/7 and separates the real threats from the false positives. The real threats are then prioritised according to their impact on your organization. The Proximus SOC will responds to these security threats through automated and manual actions and by advising your organization on how to resolve the incident. All this is supported by Proximus' MDR platform, which under the bonnet uses a Security Orchestration, Automation and Response (SOAR) solution.