CSIS
REST ASSURED

JANUARY 11, 2023

INFO SHEET

NIS2

Stay compliant with regulations and directives

SERVICES THAT HELP YOUR ORGANISATION WITH NIS2

INCIDENT MANAGEMENT

Emergency Incident Response Retainer

With our Emergency Incident Response Retainer, your organisation has access to incident response services on an ongoing basis and gets:

Emergency assistance – In the event of a cyber incident, time is of the essence. With an Emergency Incident Response Retainer in place from CSIS, your organisation can quickly access the expertise and resources it needs to respond to and manage the incident.

Tailored guidance and support – Our Emergency Incident Response Retainer gives your organisation access to our team of experts who through the retainer service are familiar with your organisation's systems and processes and can provide tailored guidance and support.

Cost savings – Our Emergency Incident Response Retainer is more cost-effective than paying for incident response services on an ad-hoc basis and you can rely on our team experts to be available 24/7.

VULNERABILITY MANAGEMENT

Active Directory Health Check

With our Active Directory Health Check, your organisation receives a 360 analysis of your Active Directory's security posture and gets:

Proactive detection – Our Active Directory Health Check identifies issues with your organisations Active Directory before they become a major problem, by providing your organisation with full a report of all current vulnerabilities and misconfigurations.

Actionable recommendations – Our Active Directory Health Check provides all the recommended actions and detailed mitigation techniques provided by our team of experts for easy adaptation and implementation.

Swiftly improved security posture – Our Active Directory Health Check is fast and provided minimum effort from your organisation. In a matter of days, you will receive a report that quickly and significantly will improve your security posture if implemented.

Continued on next page…

Continued from previous page…

Compromised Assessment

With our Compromised Assessment, your organisation receives a comprehensive overview of the security posture of your endpoints and network, and gets:

Proactive detection – Our Compromise Assessment helps prevent future cyber-attacks from occurring by addressing vulnerabilities and weaknesses in an organisation's systems. Our service identifies issues with your organisations Operating System-level security settings and misconfigurations before they become a major problem, it provides a full overview of any indicators of malware present in your organisations network, and what risks your network is exposed to that could pave the way for malicious actors to gain access.

Actionable recommendations – Our Compromise Assessment provides all the recommended actions and detailed mitigation techniques, with pin-pointed computer findings, provided by our team of experts for easy adaptation and implementation.

Swiftly improved security posture – Our Compromise Assessment is fast and provided with minimum effort from your organisation. In a matter of days, you will receive a report that quickly and significantly will improve your security posture if implemented.

GAP Analysis

With our GAP analysis, your organisation receives the foundation to build and maintain a cyber security strategy and gets:

Holistic overview – Our GAP Analysis provides a holistic overview of your organisation's performance, by identifying unknown cyber security risks, based on SANS CIS controls v8 and covering more than 150 questions.

Prioritized efforts – Our GAP Analysis provides a suggested and prioritized plan for projects that will increase your organisation's security level, aligned with efforts and budget.

Improved reputation and compliance – Our GAP analysis can help your organisation enhance compliance with relevant regulations and industry standards, improve customer trust by demonstrating a commitment to security, and better manage risks.

SECURING SUPPLY CHAINS AND IT CONTINGENCY PLANNING

Incident Response Tabletop Exercise

With our Incident Response Tabletop Exercise, your organisation gets to test and evaluate your organisation's incident response plan and procedures based on real-life scenarios, and get:

Identify weaknesses – Our Incident Response Tabletop Exercise helps your organisation identify weaknesses by testing and evaluating your incident response plan and procedures

Hands-on experience – Our Incident Response Tabletop Exercise gives your team hands-on experience by practicing their roles and responsibilities by executing the current plan with real-life scenarios.

Improved reputation and compliance – Our Incident Response Tabletop Exercise helps your organisation demonstrate its commitment to incident response and cybersecurity and assists in complying with relevant regulations and industry standards (e.g. NIS2: Securing Supply Chains and IT contingency planning)

Continued on next page…

Continued from previous page…

NETWORK SECURITY

Managed Detection and Response / Endpoint Detection and Response

With our Managed Detection and Response service, your organisation gets 24/7 monitoring for cyber threats, and gets:

Reduced risks – Our Managed Detection and Response service reduces your organisation's exposure to cyber threats with 24/7 monitoring of your systems and networks. You will have access to our team of security experts who can provide tailored guidance to increase your security posture, and when necessary, perform extensive remediation of potential attacks before they turn into full-blown security incidents.

Increased efficiency - Instead of constant in-house monitoring of security alerts your organisation can rest assured that you are protected with our 24/7 Managed Detection and Response service. Focus on your organisation's core mission and let our team alleviate the burden of the detection and response to potential threats or attacks while offering tailored advice to harden your overall security posture.

Cost savings – Many organisations dealing with a critical security incident have been breached unknowingly for months. Having our Managed Detection and Response service can reduce the risk of a full-blown security breach by detecting potential indicators of attack quickly and effectively. If a breach does occur, our team will quickly identify and remediate the threat, minimizing the impact on your organisation's operations and reducing any downtime or loss of productivity.

Cyber Defence Feed

With our Cyber Defence Feed, your organisation gets comprehensive visibility into malicious domains and IP addresses, and gets:

Block malicious web content – The Internet is becoming an increasingly bigger security threat, with more than 22% of all new domains created for illegal purposes. Your employees' day-to-day use of the Internet presents a challenge because it is impossible for ordinary users to tell which sites are safe. For example, malicious code is often found in banners on entirely legitimate websites.

Prevent data leakage – Our Cyber Defence Feed will not only help prevent internet-based exploits and malware downloads, but it can also mitigate communication from existing malware intrusions and prevent them from leaking data. This can be accomplished by implementing the corresponding rules in the on-premise security solution.

Detect advanced malware – our Cyber Defence Feed can help detect advanced malware that is managed to infect network devices by circumvention of locally deployed security products. This happens because the feed data does not rely on signatures or behavior but reveals the infrastructure that the malware attempts to communicate with.

Find out how we can help your organisation as well

call us +45 8813 6030
or visit www.csis.com/nis2