WHITE PAPER

NIS 2 Directive

ANOMALI

Synopsis

In this white paper, Anomali puts into context why the EU and national security agencies like the UK NCSC have acted through NIS2 and CAF to mandate that robust cyber security threat and risk understanding coupled with effective measures to protect, detect, and respond are established and sustained in effective operation. Cyber threats and attacks now pose full-on business interruption risks, the impact of which for operators of essential services and the nations they serve are huge – the stakes are too high. In truth the stakes are too high for the majority of all organizations so this guidance is applicable everywhere. At its heart is the principle of threat-led security operations founded on 3 areas of grip. This also covers Anomali's approach to bringing CTI and SOC teams to elite levels of operation and providing CISOs and stakeholders with the assured confidence that the mandates are being met.

NIS2 Directive with CAF from the NCSC

Organizations have digitally transformed at a frenetic pace over the last several years. Driven by three factors: (1) the pace of technology advances (e.g. Cloud/SaaS); (2) the proliferation of B2B and B2C marketplaces; and (3) the Covid pandemic that put the foot firmly to the floor on the above and added adoption of fully remote and hybrid working just to spice up the mix.

It is fair to say now that organizations are wholly dependent on their networked IT/OT and internet-facing services and interfaces to operate and grow.

Before this, CISOs' major concerns were governance and compliance-driven. For information security, this is centered on data privacy. Operationally the majority of threats were website defacements, denial of service, fraud, and phishing.

Now, governance and compliance have not gone away. The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. NIS2 has expanded the scope of entities covered, states why these entities are in scope and so more clearly shows the way to more effective security in terms of resilience and incident response. 'Preparedness' is the fundamental theme – both at a national and entity level.

In addition, how compliance is evidenced has also changed. It is now done continuously, and the standards demand an analytical approach based on real security data that evidence the efficacy of security controls and posture concerning an understood and monitored threat environment.

The bigger concern today is that a cyber-attack can stop the business running. Halt its ability to earn and grow. And, if this business is part of the digital and/or critical fabric of society it can have a potentially catastrophic impact at a regional and national level. NIS2 has been designed to lay out the expectations of both Operators of Essential Services (OES) to achieve the outcomes specified by NIS and the role of Competent Authorities (CA) in assessing the extent to which OES are achieving those outcomes.

Cyber risk has become a full-on business interruption risk and so sits squarely at the board level. The board and its risk committee need the assurance that these threats and risks to business operations and growth are properly understood with proportionate mitigation in place to bring the risk within the appetite of the organization. Moreover, compliance insists that they are properly informed, making proportionate decisions, and establishing adequate security operations.

So, whether or not you are an OES, any organization with a high dependence on its digital infrastructure would do well to be guided by NIS2. The UK NCSC (National Cyber Security Centre) has worked with the UK government to define the Cyber Assessment Framework (CAF) enshrining "Indicators of Good Practice" (IGPs).

There are 4 CAF Objectives:

- **CAF Objective A** – Managing Security Risk
- **CAF Objective B** – Protecting Against Cyber Attack
- **CAF Objective C** – Detecting Cyber Security Events
- **CAF Objective D** – Minimizing the Impact of Cyber Security Incidents

What the NIS2 Directive and CAF from the NCSC are asking for can be enshrined in one word - "Grip". The drive is very much towards the realities of securing and protecting organizations and so goes beyond risk management.

Many board-level risks change relatively slowly, only needing assessment quarterly, biannually, or even annually. Cyber risk is exceptionally dynamic and it demands relentless grip across three key areas (below) – each of which features in NIS2 and its Cyber Assessment Framework (CAF). The NIS2 directive now enshrines the unifying principle of Threat Led Security Operations bonding relevant Threat Intelligence to the crucial areas of resilience, preparation, and active defense:

Grip #1 - Threat Landscape

What visibility do we have into the 'what' and 'why' of threats?

What's at risk?

What are the key trends?
(NIS Objective C – Detecting Cyber Security Events, CAF C1.D – Identifying Security Incidents)

Grip#2 - Security Posture

How protected/prepared are we?
(NIS Objective B – Protecting Against Cyber Attack, CAF B5.A – Resilience Preparation)

Have I optimized my security operations?
(NIS Objective D – Minimising the Impact of Cyber Security Incidents, CAF D1.A – Response Plan, CAF D1.C – Testing & Exercising)

Am I reducing the attack surface?
(NIS Objective B – Protecting Against Cyber Attack CAF B5.A – Resilience Preparation)

Do I have immediate, actionable visibility?
(NIS Objective C – Detecting Cyber Security Events, CAF C1.A – Monitoring Coverage)

Grip#3 - Actualized Threats

Can I detect and respond at the pace of any incident?
(NIS Objective C – Detecting Cyber Security Events, CAF C1.C – Generating Alerts, CAF C2.A – System Abnormalities for Attack Detection)

Can I minimize harm and disruption to the business?

This is good news. This is compliance that drives more effective outcomes for businesses and wider society. So, what should organizations do with the new NIS2, CAF, especially with regard to its asks on intelligence-led security operations?

Let's take each of the relevant CAF sections in turn.

NIS Objective B

Protecting Against Cyber Attack, CAF B5.A – Resilience Preparation

This is an uncompromising drive towards relevant threat intelligence making a difference in how the organization has prepared. To quote Sun-Tzu's Art of War – "If you know neither the enemy nor yourself, you will succumb in every battle." It is not enough to have figured out your threat landscape. It is not enough to have deployed the traditional set of security tools across your digital infrastructure. It is about applying the knowledge of how these adversaries are likely to attack and knowing what opportunities are available to them across what they can see – the attack surface. Combining that with preparing security operations, allied to the business' operation establishes a resilient, dynamic, and adaptable Security Posture. One where the SOC can be fully proactive and get beyond the 'whack-a-mole' reactive, alerts ticket factory they most often find themselves in.

Anomali addresses this area head-on. Through the combination of the Anomali Intelligence Channels for Malware, Botnets & C2, Vulnerabilities and Exploits, Adversary Monitoring, Phishing & Fraud, and the analysts' assistants through an Anomali Copilot, relevant intelligence can be extracted and immediately bonded to security operations across protect, detect, and respond as well as prioritizing attack surface reduction and threat hunting.

> "You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware."
> - IGP

NIS Objective C –

Detecting Cyber Security Events, CAF C1.A – Monitoring Coverage

With Anomali, once you have bonded Threat Intelligence with Security Operations you can automate the sending of relevant IOCs down to the front-line security controls, gain immediate visibility of any detections, and through this automation, free the SOC analysts to contain the threat, disrupt the attack and minimize the harm to the business and customers. That's mission achieved for the security team.

> "You easily detect the presence or absence of IoCs on your essential services, such as known malicious command and control signatures."
> - IGF C1.a

NIS Objective C – Detecting Cyber Security Events, CAF C1.C – Generating Alerts, CAF 1.D - Identifying Security Incidents, CAF 1.E - Monitoring Tools and Skills, CAF C2.A – System Abnormalities for Attack Detection)

> "A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts."
> - IGFC1.c

> "You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare)."
> - IGF C1.d

You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.
- IGF C1.d

You receive signature updates for all your protective technologies (e.g. AV, IDS).
- IGF C1.d

You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).
- IGF C1.d

“Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.”
- IGF C1.e

“System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.”
- IGF C2.a

The Anomali platform sources and curates the widest range of open-source and commercial threat intelligence worldwide. Anomali works directly with its customers to identify and source the most relevant intelligence and also enables its analysts to rapidly acquire new intelligence from advisories, research, news, and intelligence-sharing communities. Through Anomali this intelligence is instantly bonded to an organization’s security tools’ telemetry providing a scope, scale, and velocity of detection and analytics that is unrivalled. This puts the organization fully on the front foot – whether that’s to spawn a more detailed investigation, to instantly update their security posture and protection, or to get immediately out and ahead of an attack.

NIS Objective D – Minimising the Impact of Cyber Security Incidents, CAF D1.A – Response Plan, CAF D1.C – Testing & Exercising)

“Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen.”
- IGF D1.a

“Exercise scenarios are based on incidents experienced by you and other organizations, or are composed using experience or threat intelligence.”
- IGF D1.c:

The IGFs in Objective D encourage organizations to use externally sourced relevant intelligence bonded to their own experience of incidents and attacks. That enduring and rich knowledge base gives visibility and hence focus to the business and the security teams to be able to work together to ensure the business’ successful and secure operations and growth. The organization can be confident they are at the very best state of preparedness and resilience for threats and attacks they may face. For the business, this means they can operate and grow with confidence, and for the security teams, they gain pride and knowledge that they are operating at the elite level.

Taking all of the above together underlines the need for a platform that enables achieving these outcomes end to end – establishing a dynamic and amplifying cycle of security operations. Anomali stands out as a platform that does just this for customers and in so doing increases the ‘Return on Security Investment’ (RoSI) across an organization’s security tooling, reduces cost, and most importantly establishes and sustains the security teams grip, relevance and partnership with the wider business which is fundamental to the success of all modern digital enterprises.

ANOMALI