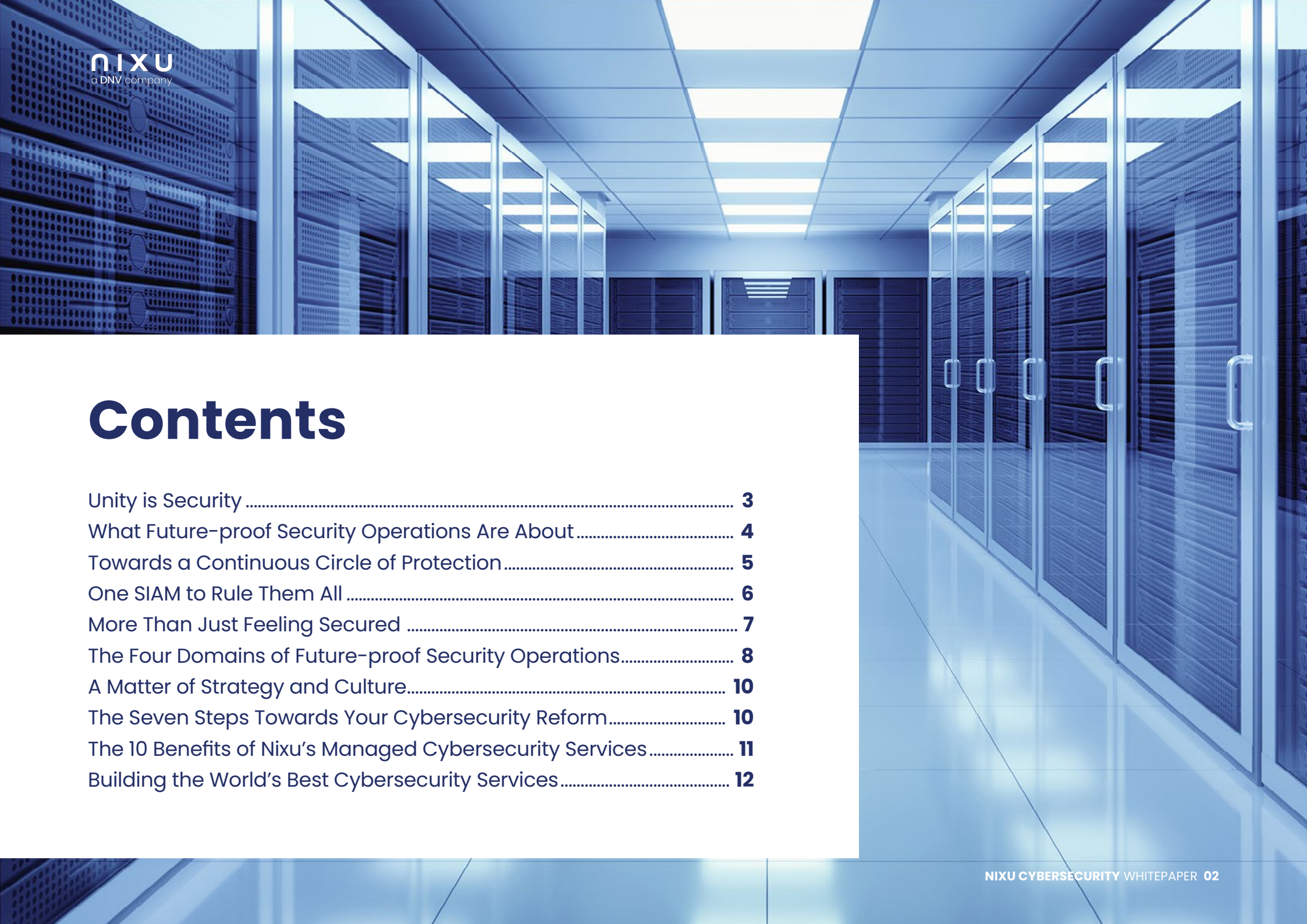
nixu
a DNV company

FUTURE-PROOF SECURITY OPERATIONS

What's Your Most Important Security Procedure and How to Create It

WHITEPAPER 03/2024



Contents

Unity is Security

As a Chief information Security Officer (CISO) or business director, you do not want to hear that a data breach has occurred. What you want to hear is that an attempted breach was detected but no damage has materialized, as active countermeasures were applied, and protective measures have been applied to prevent that attack vector in the future.

The problem is that no current cybersecurity operation can match the attackers' pace – not one of them.

Sure: you have compiled corporate security guidelines, everything from servers to workstations and in between has been protected, the Security Operations Center (SOC) does its job, and you get the alerts. However, the identification, protection, detection, and response processes are siloed. There is no connection to develop your protection through detection, i.e., opportunities to keep learning from the evolving cyber-attack tactics and thus prevent them more efficiently. Consequently, security operations are divergent instead of unified, and reactive instead of proactive. Taking corrective actions is slow. Concurrently, managing cybersecurity costs and vendors has become harder than it should be. What once felt secured suddenly does not. The root cause of this phenomenon lies deeper than simply the technologies.

As a company on a mission to keep digital society running, we have decided to speak out and help you take a better route – a path less traveled. In this white paper, we'll take a look into the unified future of cyber security, from reactivity to proactivity and a cultural reform.

Now, let's take a time leap in the future of cybersecurity and start the fusion of people, processes, technologies and data.

Yours truly,

Jan Mickos
Managed Services Director
Nixu Corporation

"No current security operation can match the attackers' pace."

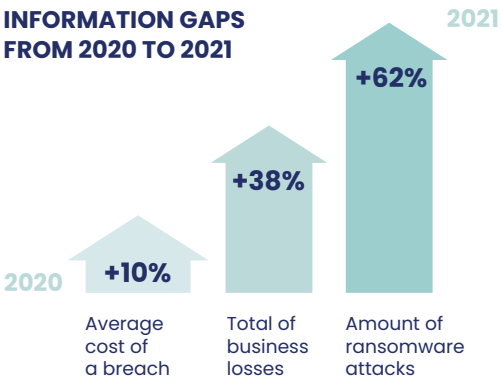
nixu
a DNV company

What Future-proof Security Operations are about

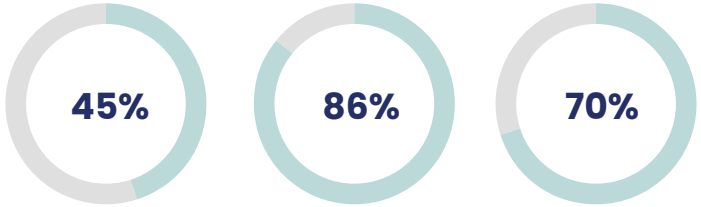
It still takes an average of 287 days for an organization to identify and contain a data breach. The effects of the information gaps between security operations are clearly visible in numbers: the average costs of a breach have increased 10% from 2020 to 2021. Total business losses have increased by 38%. At the same time, there has been a 62% increase in ransomware attacks, and 15M DDOS attacks are estimated for 2023. A total of 45% of breaches involve hacking, 86% are financially motivated, and 70% are caused by outsiders. Are we losing the battle?

In addition to attackers continually improving their techniques and tactics, the effects of the pandemic and complexity of hybrid environments, geopolitical issues now set a new pace for rapid change. Detection and response are simply not enough for keeping up with the threat landscape, and responding to this takes a lot more than new technology or a security operations center. In fact, the SOCs of today are glorified alarm systems that lack the continuous security posture improvement capability that is needed. Thus, we need to start redefining cyber security operations through a cultural reformation and adapt cybersecurity as a part of the strategy.

THE IMPACTS OF THE INFORMATION GAPS FROM 2020 TO 2021



ANATOMY OF THE BREACHES



nixu
a DNV company

Towards a Continuous Cycle of Protection

Future-proof security operations consist of four elements: identify, protect, detect, and respond. Now, think of these established on separate islands for protecting your business. They were once set for one specific target, based on the best possible view of the current threats, however the enemy is changing its strategies all the time and learning from you. As the next attacks occur, they won't actually hit the islands, which are easier to defend, but the required service traffic between them. To succeed in their common tasks again and again, the islands need to deliver information and support each other.

For example, if you want a database or service to be safe, it should be added into a security program based on its lifecycle. The protective operations then help to ensure that nothing happens, and if something happens, it is detected and addressed appropriately. Above all, situational awareness arises from identification. The entire process is run through a coherent security operations platform, agilely coordinating the four domains and helping you prepare for the attackers' next move.

MODERN SECURITY OPERATIONS

Based on NIST Cybersecurity Framework

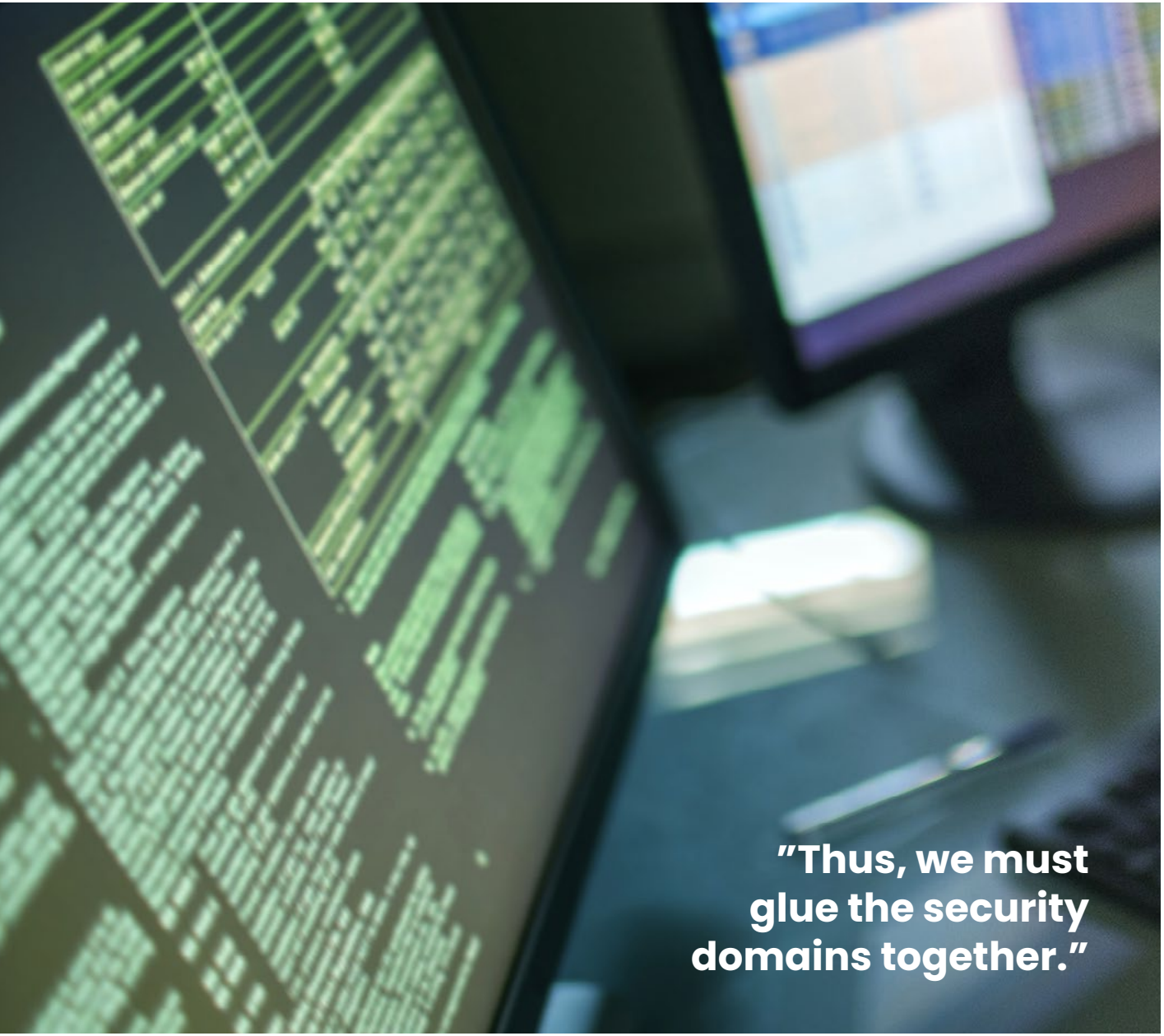
"In fact, the SOCs of today are glorified alarm systems."

nixu
a DNV company

One SIAM to Rule Them All

In a real-life hybrid business environment, the four domains – identify, protect, detect, and respond – involve an endless list of service providers and technologies from cloud applications to local server rooms and beyond. The truth is no one has had the willingness or competence to take full responsibility. **Thus, we must glue the security domains together**. This enables the first true Security SIAM (Service Integration and Management).

"The truth is no one has had the willingness or competence to take full responsibility."



More Than Just Feeling Secured

To take concrete actions instead of making assumptions, you need a centralized channel responsible for managing security operations. This channel creates and implements new types of security tactics by gathering information from several sources and delivering it to all the parties included.

For example, after Identify completes an analysis of an attack, it sends the new signatures to be added to network providers’ Detection sensors, then the Protection updates are ensured in the operating systems for blocking the dangerous command inputs, and that Response creates the host-specific rules for filtering the traffic from particular channels. The process is agilely repeated in accordance with all the four domains. It is never considered ready, but developed and further automated all the time, attack by attack.

nixu
a DNV company

The Four Domains of Future-proof Security Operations

Identify

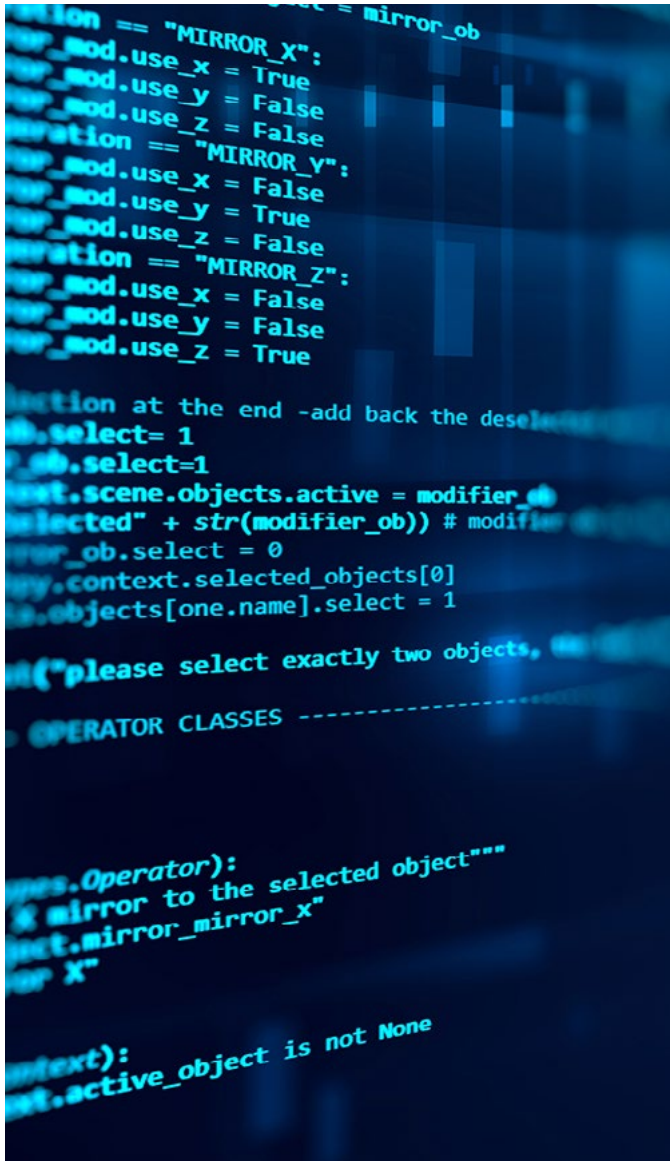
The Identify domain continually assesses the business risks related to gaps in cybersecurity, based on relevant and actionable Threat intelligence. This helps maintain situational awareness of global threat landscape development, integrate it to your business environment, and thus, drive informed decisions. Threat intelligence means you understand what is happening and whether it will affect your systems. The domain constantly evaluates and reduces the internal attack surface by asset and Vulnerability Management, offering threat modeling to align with organizations' business and operational goals.

Protect

The Protection domain continually manages the cybersecurity posture across the hybrid IT business environment. It uses security tools to prevent malicious events in Endpoints and Networks, and constantly improves resiliency of the environment by ensuring the ICT components are hardened and the attack surface is reduced through segmentation and segregation. The SOC collects data as a feedback loop to further improve protection. Also, it ensures that Security Posture Management is a cross-domain function.

Detect

Detection establishes and maintains security operations and a 24/7 capability to detect and investigate threats efficiently and continuously. It offers a comprehensive detection capability over different ICT domains, ensures coverage to all business-critical value streams, Application Security Monitoring (AppSOC) and Operational Technology (OT). The detection function is combined with an automated reaction capability to mitigate anomalies 24/7 without delay.

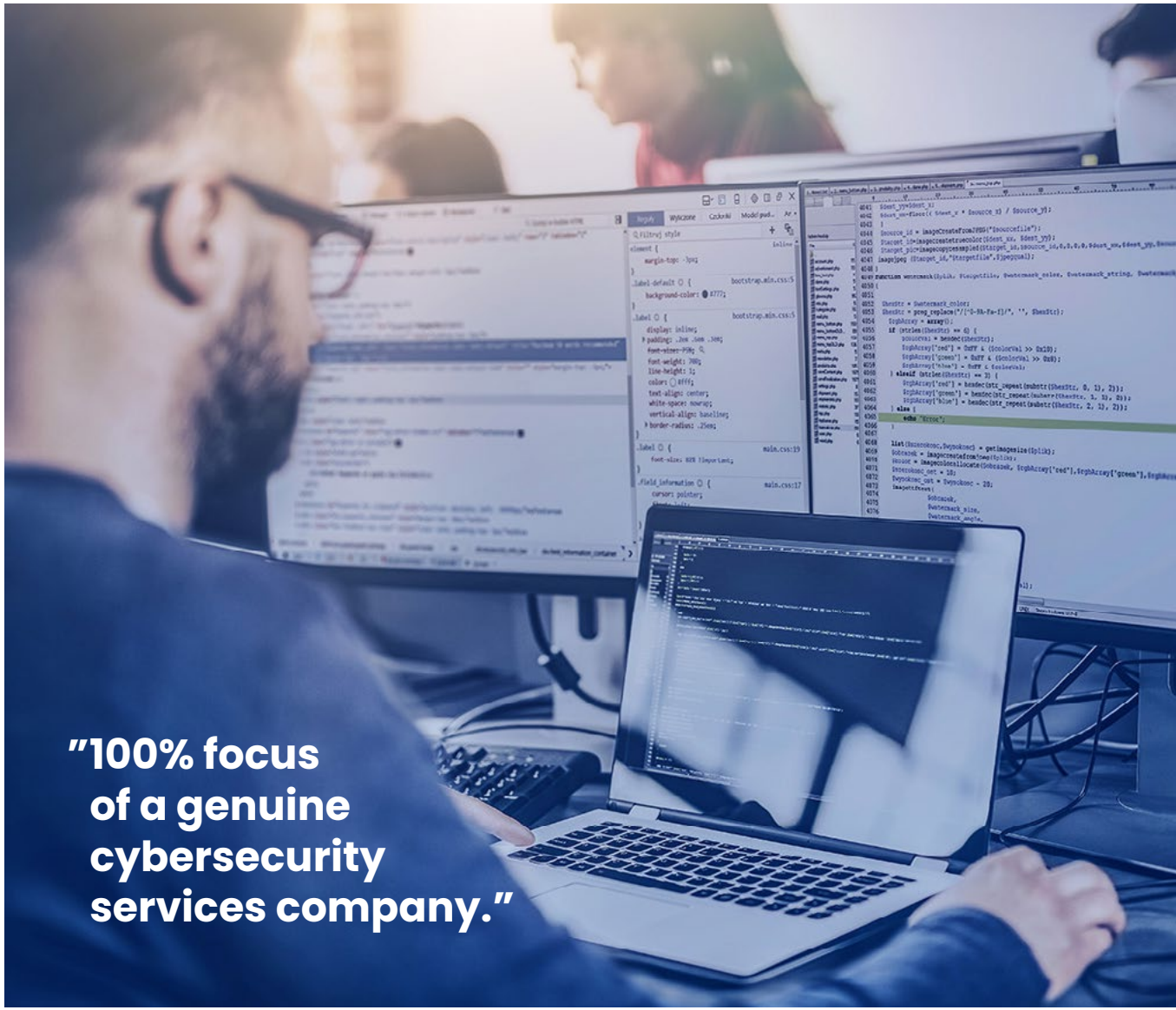


Respond

Respond establishes and rehearses incident response and recovery capabilities. Reduced effects are built through an automated and semi-automated multilayer Response capability to contain and mitigate anomalies with pre-agreed procedures and technical operations. The aim is to plan and practice quick response scenarios on several domains, such as networks and servers, to ensure minimum downtime after major incidents.

The role of SOC service

SOC ensures the Detection and Reaction capabilities. At Nixu, our differentiators are Mitre Att@ck Detection Capability, 24/7 Analysis by the Security Subject Matter Experts, Incident Response backed by the Nixu DFIR team (Digital Forensics and Incident Response), and Security Incident Manager. We currently scale the SOC services for 50+ clients, with 100+ people and 100% focus of a genuine cybersecurity services company.



nixu
a DNV company

A Matter of Strategy and Culture

Future-proof security operations are a value-creating aspect of your individual business strategy and cybersecure culture. Thus, these operations are implemented in a different context than, for example, budgeting a single feature, such as a security client, or choosing a group of technologies. This manifests through a change in security operations, responsibilities, and ways of working.

Cybersecurity reform begins with people's readiness for change, and now is the time to start. Organizations everywhere in the world are challenged to act faster and in a more humane way. As societies, businesses, and human beings, we've faced the crisis, seen how the global operating environment can change in days, and embraced the new ways of working. What everyone wants is stability and true meaning for their work – a purpose and a mission – and that's exactly what future-proof security operations are all about. It changes the people's behavior through security knowledge and understanding.

It's a concrete, accurate and continuous process that helps people take advantage of new technologies and practices and thus, develop themselves professionally. Technology itself isn't the same as cybersecurity capability. The process uses the technology to enable it. As the operations are modernized, the true and daily needs are met. Also, the times of cybersecurity doing its job in an isolated domain are long gone. Now is the time to start a dialogue between the cybersecurity domains and business representatives to modernize daily security operations.

THE SEVEN STEPS TOWARDS YOUR CYBERSECURITY REFORM

1. Build understanding of critical business streams/processes.
2. Map technical components needed to operate business stream.
3. Align situational awareness of internal components and external threat landscape (Identify) with the technical components.
4. Ensure that the technical component settings and vulnerabilities are assessed and risk of anomalies is reduced (Protect).
5. Align Detection and Response capabilities of technical components with detailed accuracy ensuring threats are being detected and anomalies responded to.
6. Build a continuous practice to maintain the alignment & mapping = enable Security Fusion.
7. Communicate & Collaborate with business stakeholders by elaborating their level of problems to security features and capabilities.

At Nixu, this is what we help you do. We call it Managed Cybersecurity Services.

nixu
a DNV company

THE 10 BENEFITS OF NIXU'S MANAGED CYBERSECURITY SERVICES

1. Proactivity instead of reactivity: better security, fewer risks, clear results, and impact.
2. Faster reaction times: reduced costs due to data breaches.
3. Better readiness for change and crisis situations: centralized development functions are managed efficiently, continuous improvement of security functions and technology. Up-to-date information and administrative and operational efficiency speed up decision-making and improve predictability.
4. Peace of mind for CISO and business representatives: responsibility outsourced, managing the vendors becomes easier.
5. Aligned with business priorities.
6. Faster security innovations: more competitive advantage and ensured brand value.
7. Fewer risks: functions and features are iterated step by step.
8. Clear responsibilities and more motivation for security: with the different parties learning from each other and having a common goal, security and success increases, and the risk for unprofitable investments decreases.
9. Concrete actions that ensure the safe implementation of the business strategy: a holistic approach to cybersecurity.
10. Safer business ecosystems: new partners can join in a standardized platform.

Building the World's Best Cybersecurity Services

Nixu represents the future of managed cyber-security services. We combine cyber intelligence with the best expertise and responsiveness to keep your business protected.

- **Responsiveness:** whenever you need us, we are here to help.
- **Expertise:** advanced services and the best cybersecurity expertise – at your service, 24/7.
- **Future-proof:** continuous fusion of people, processes, and technologies with data as the driving force.

Our Managed Cybersecurity Services in Numbers:

- Incidents detected and responded to in **~12** minutes.
- Incidents are solved by security analysts **24/7.**
- **250+** solved Digital Forensics and Incident Response cases a year.
- **100+** experts focusing on Managed Cyber-security Services.
- **250+** Incident Response cases solved in 2021.

nixu
a DNV company

Nixu, a DNV company, is a trusted cyber security services partner. We help our customers ensure business resilience with peace of mind across multiple industries, enabled by some of the best cyber security professionals in Europe.

For more information, visit: www.nixu.com.

Nixu Corporation
Nixu Corporation
@NixuCorporation
@NixuCybersecurity

nixu.sales@nixu.com
nixu.com