NOESIS

Technology for real growth

eBook

Top 10 Cybersecurity capabilities for it leaders

The guidelines and investment priorities to secure a resilient cybersecurity roadmap.

Contents

Cybersecurity: You've been warned! 4

Top Security Challenges Facing CIO's 5

Security by design 6

Key priority area 7

Time to define your Roadmap 9

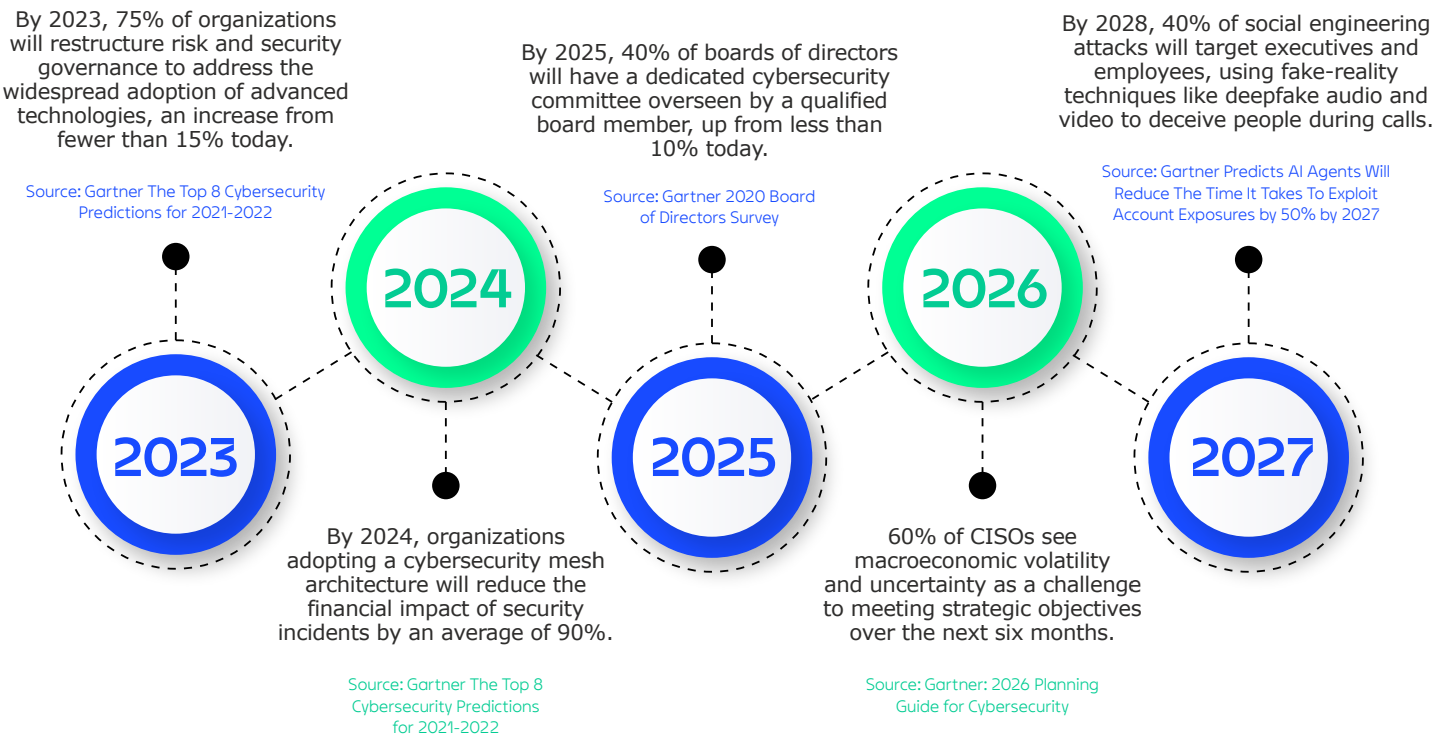
executive summary

In today's rapidly evolving digital world, cybersecurity is no longer just an IT concern; it is an imperative business need. IT leaders are battling an ever-growing wave of sophisticated threats, such as ransomware, phishing, and supply chain attacks, which can disrupt operations, compromise sensitive data, and damage reputation in an instant. Add to that the complexity of hybrid and cloud environments and the challenge of managing identities and access, and it becomes clear that traditional security approaches are no longer sufficient.

This ebook, drawn from Noesis' experience, reveals the top 10 cybersecurity capabilities that all IT leaders need to master. From cutting-edge threat detection powered by AI to Zero Trust network security and Extended Detection and Response (XDR), these technologies are reshaping how organisations defend themselves, offering integrated, real-time protection for data, applications, networks, and devices.

But technology is only part of the equation. Building a resilient cybersecurity roadmap that aligns with your business objectives is crucial to innovating boldly, acting quickly, and minimizing risk. This guide is your strategic compass for navigating the complex cybersecurity landscape with confidence, helping you avoid fragmented, reactive solutions and empowering you to build a future-ready defence.

Cybersecurity: You've been warned!



Cybersecurity outlook

It's time for organizations to refocus their strategy and reassess the critical aspects of the security architecture and empower themselves in a structured way with cutting-edge services and technologies to safeguard against increased cyber-exposure and insider threats.

José Gomes

IT Operations, Cloud & Security
Associate Director at Noesis

The current context poses a huge challenge to IT departments and has also been an impetus for a change not only in mentality, but also in prioritization and investment, when it comes to cybersecurity.

Nuno Cândido

IT Operations, Cloud & Security
Associate Director at Noesis

Top Security Challenges Facing CIOs

Escalating Cyber Threats

Ransomware-as-a-Service, phishing, and supply-chain attacks are on the rise, with attackers now faster, more automated, and better funded.

Impact: Business disruption, data loss, reputational damage.

Cloud & Hybrid Complexity

Multi-cloud and hybrid environments increase the attack surface, with misconfigurations continuing to be the leading cause of cloud breaches.

Impact: Reduced visibility, inconsistent security controls, shared-responsibility confusion.

Identity & Access Management

Managing identities across employees, contractors, partners, APIs, and machines is increasingly complex, with stolen credentials remaining the leading breach vector.

Impact: Privilege abuse, lateral movement, insider threats.

Data Protection & Privacy

Sensitive data resides across multiple environments, while regulatory requirements such as GDPR, NIS2, DORA, and HIPAA intensify compliance pressure.

Impact: Regulatory fines, legal exposure, loss of customer trust.

Talent & Skills Shortage

A shortage of skilled cybersecurity professionals' forces CIOs to balance talent retention with 24/7 security operations running.

Impact: Overworked teams, increased risk, reliance on external providers.

Tool Sprawl & Poor Integration

An overabundance of poorly integrated security tools generates high volumes of low-context alerts, overwhelming teams and slowing response.

Impact: Slower incident response, missed threats, inefficiency.

Limited Visibility & Observability

Conventional security approaches lack holistic, real-time visibility, limiting the CIO's ability to correlate operational performance, security posture, and business outcomes.

Impact: Reactive security posture, delayed detection (high MTTD/MTTR).

Securing Remote & Hybrid

Remote endpoints and unmanaged devices increase exposure beyond the corporate perimeter.

Impact: Endpoint compromise, data leakage.

Third-Party & Supply Chain Risk

Third-party vendors and service providers can act as gateways for cyberattacks, while CIOs often have limited visibility into their security maturity.

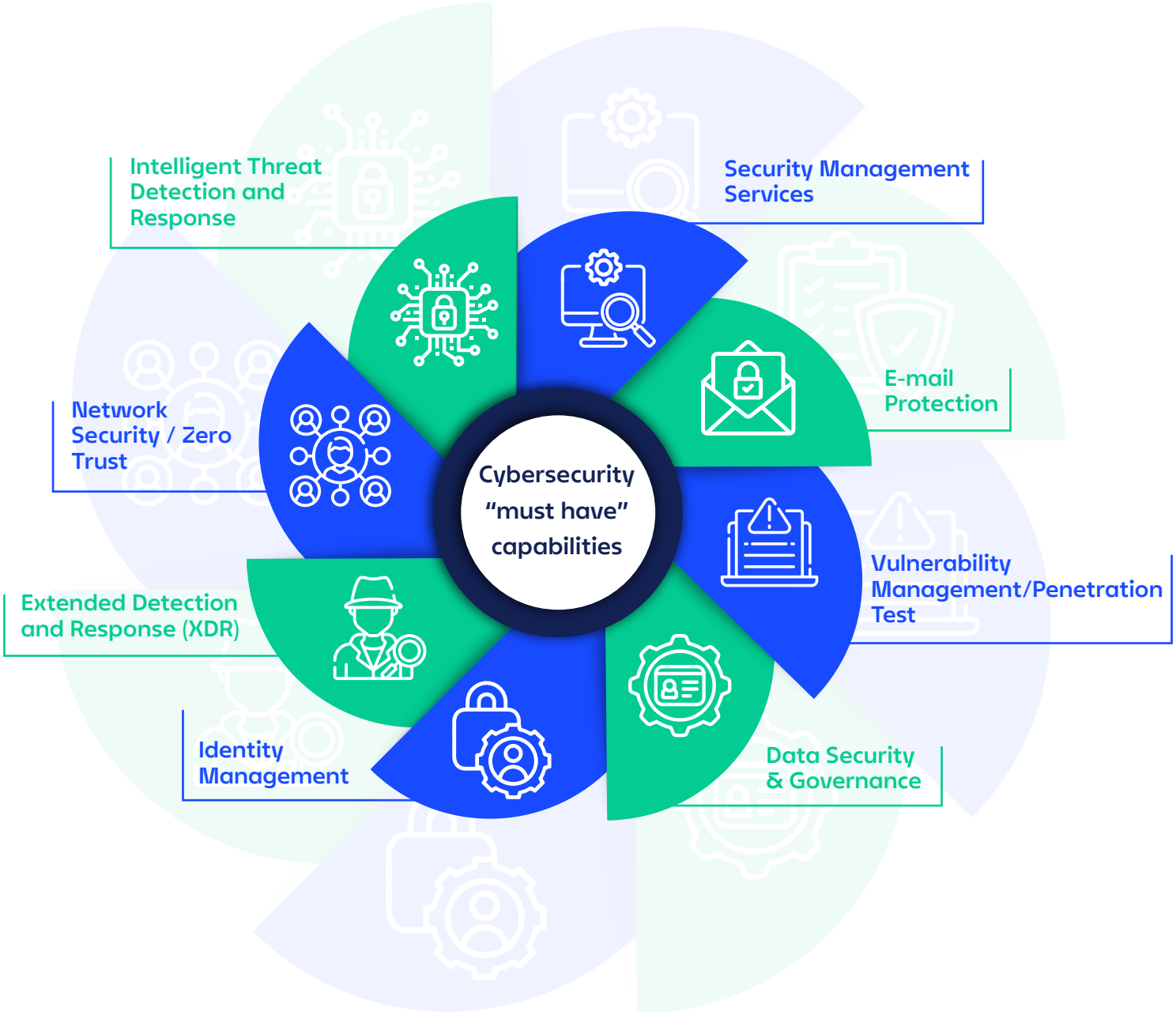
Impact: Indirect breaches, contractual and compliance risks.

Aligning Security with Business

Security is not yet fully embedded as a business enabler, forcing CIOs to constantly trade off speed and innovation against cost and risk.

Impact: Shadow IT, security bypasses, business friction.

Security by design



Key priority areas

Intelligent Threat Detection and Response

- Self-learning AI swiftly stops cyber-attacks, including ransomware and phishing
- Detects, investigates, and responds to emerging threats instantly
- Safeguards cloud environments from unprecedented cyber threats

Key technologies

DARKTRACE

Extended Detection and Response (XDR)

- It detects and responds to threats across endpoints, networks, and applications
- Unifies data from multiple security tools
- It improves visibility and simplifies threat management

Key technologies

paloalto NETWORKS · CROWDSTRIKE · Microsoft · CHECK POINT

Network Security / Zero Trust

- Securing all physical and logical devices
- Applying Zero Trust principles
- Essential for countering network threats like worms, viruses, and hackers

Key technologies

paloalto NETWORKS · zscaler · FORTINET · CHECK POINT

Identity Management

- Identity management ensures the right people access the right resources
- It verifies user identities and controls permissions
- Cover service, app, root, and priviledge accounts across the organization

Key technologies

Delinea · Microsoft · Saviynt · CYBERARK

Data Security & Governance

- Leverages AI to protect sensitive data and ensure compliance with regulations
- It automates threat detection, risk management, and policy enforcement
- By enhancing visibility and control, AI helps organizations mitigate risks and maintain data integrity

Key technologies

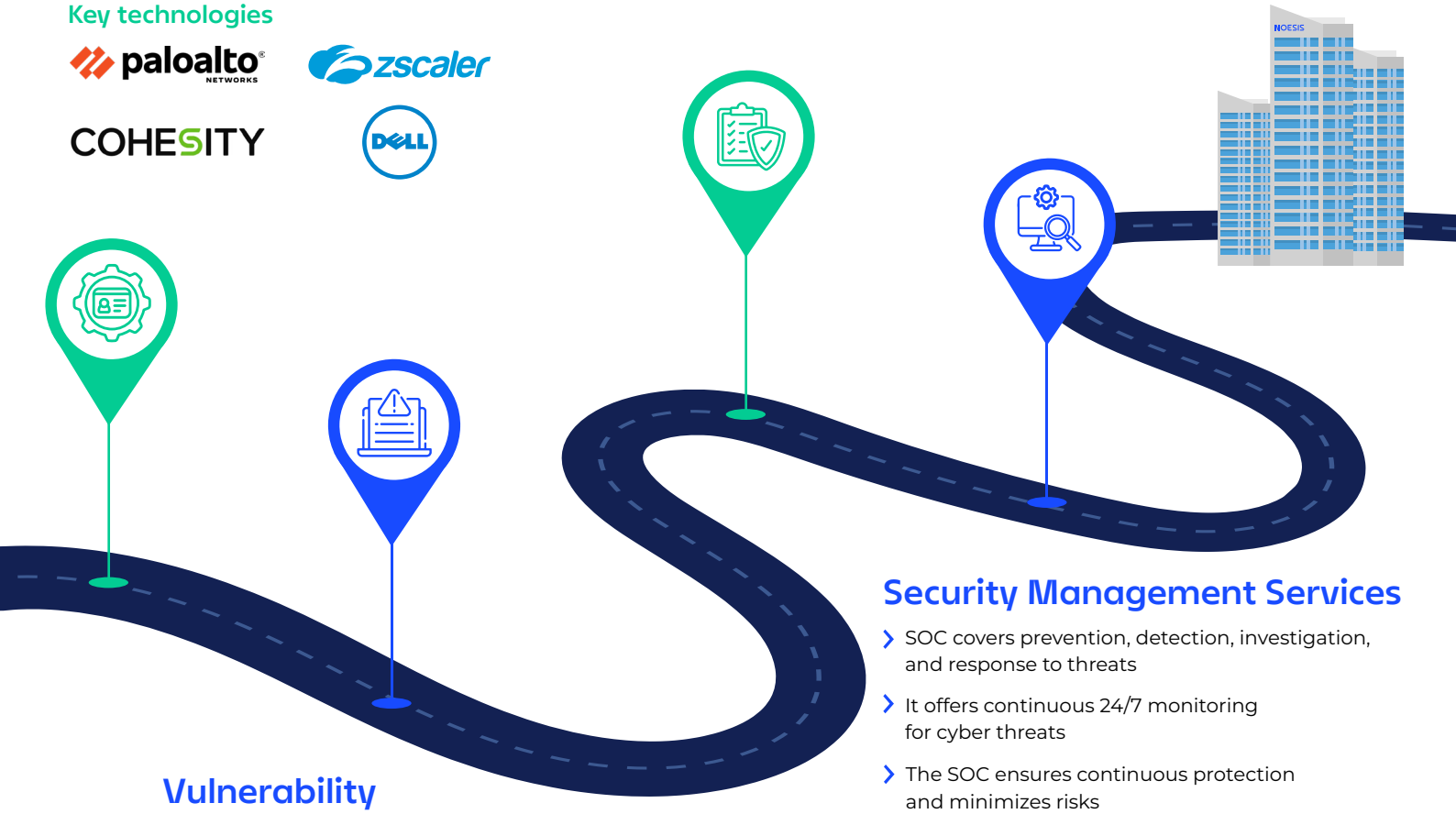
paloalto NETWORKS zscaler COHESITY DELL

E-mail Protection

- Identifies phishing, malware, ransomware, and business email compromise (BEC) using signature-based and behavioral analysis
- Scans links and attachments in real time to block malicious content before users interact with it
- Detects compromised accounts, spoofed domains, and executive impersonation through anomaly detection and identity-based controls

Key technologies

CHECK POINT DARKTRACE



Vulnerability Management/Penetration Test

- Identify and assess security weaknesses
- Prioritize risks and apply fixes to reduce exposure
- Mitigate inappropriate and risky access

Key technologies

tenable DARKTRACE

Security Management Services

- SOC covers prevention, detection, investigation, and response to threats
- It offers continuous 24/7 monitoring for cyber threats
- The SOC ensures continuous protection and minimizes risks

Key technologies

CROWDSTRIKE Microsoft paloalto NETWORKS FORTINET

Time to define Your roadmap

Starting this cybersecurity roadmap may seem challenging, especially when doing it alone.

Make sure you get proper guidance and counseling to guarantee you start off on the right foot and scale in the right way.

Our expertise tells us that many companies are reacting ad-hoc and end up investing in a distributed way, solving specific needs but do not guarantee real-time holistic protection of organizations' data, email, applications, assets, and networks, from sophisticated attacks.

Pro Tip

Do not rush, plan and prioritize security investments!

Would you like to know what's the right move for your business?

Free Content | Government institution reduces threat analysis time by 92%!
Secure and control all privileged accounts across your enterprise

Contact us and we'll guide you throught this journey

NOESIS

www.noesis-corporation.com

eBook