HADRIAN

Your First 90 Days
A CISO Transition Guide

EBOOK

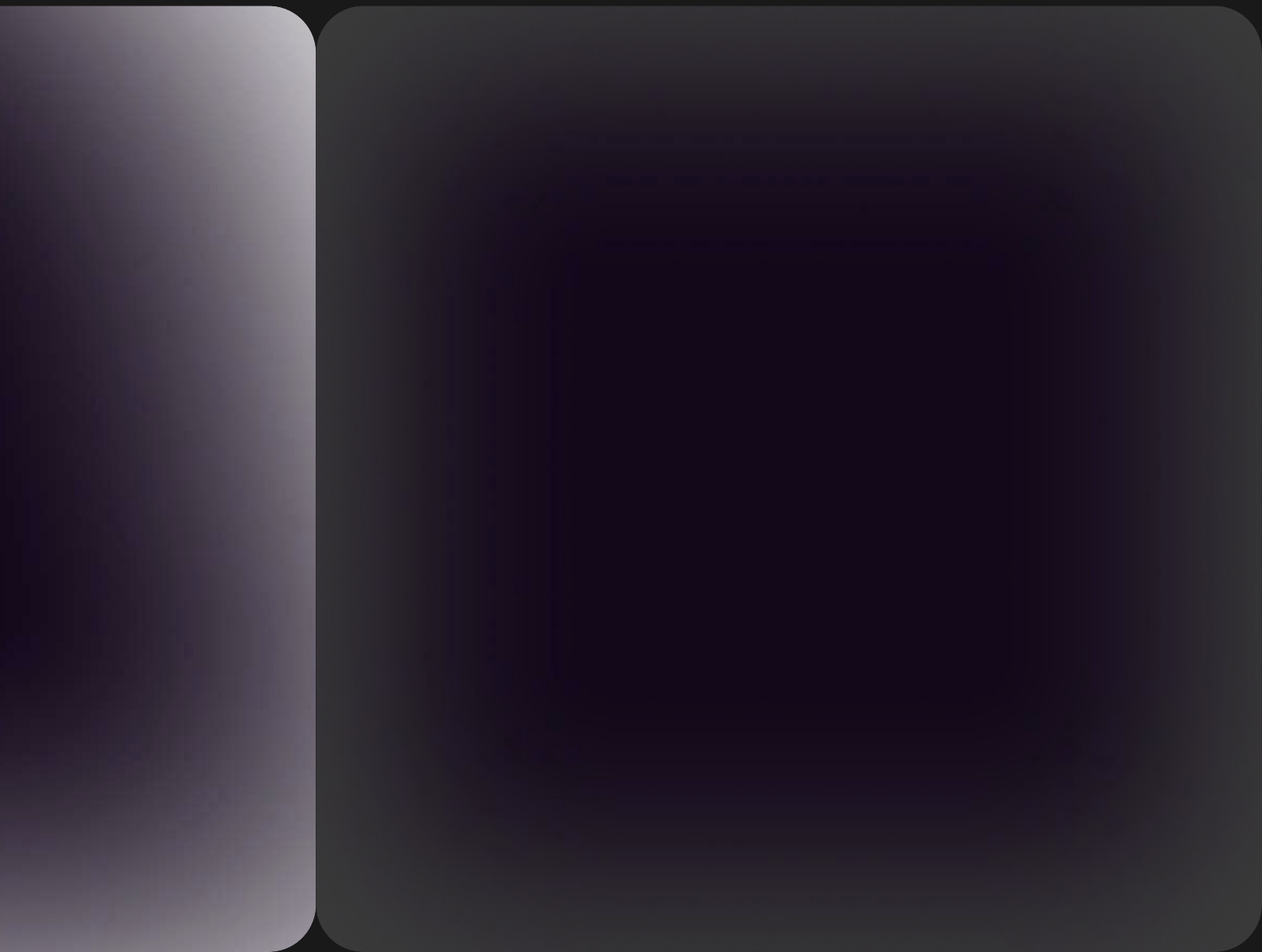


Table of Contents

Introduction

Transitioning into the role of a Chief Information Security Officer (CISO) in a new firm is challenging due to its extensive responsibilities. Assuming the CISO post of a new organization involves managing a totally different security infrastructure, ensuring regulatory compliance, and aligning security with business strategies. Staying updated on emerging threats and understanding the organization's technology landscape adds complexity. Building credibility with stakeholders like executives and IT staff is essential, requiring strong communication and leadership skills.

Balancing immediate security needs with long-term goals, especially in resource-constrained environments, further complicates the transition. Each company’s unique culture and attitude toward risk necessitate quick adaptation. Resistance to change may also arise, making it crucial for the CISO to align security initiatives with business objectives.

Management guru Michael D. Watkins brought forward the concept of a three-month transition into a new leadership role in his book "The First 90 Days: Proven Strategies for Getting Up to Speed Faster and Smarter". Based on insights from over 200 CISOs, Hadrian’s "The CISO’s First 90 Days: A Transition Plan for Success" offers a structured framework for new CISOs.

This plan provides specific goals, metrics, and phases to ensure a smooth transition, focusing on assessing security maturity, identifying improvement areas, implementing changes, and demonstrating progress. This 90-day plan is designed to help CISOs navigate challenges and make a significant impact early on.

Adapting the 90-Day Plan

The first 90 days in a new organization are crucial for a CISO for several reasons. This period aligns with quarterly business cycles, offering a structured timeframe for setting and achieving initial goals, and allows for natural acclimatization. It's a key opportunity for securing early wins that build credibility and momentum, laying a foundation for long-term strategic planning.

The 90-day plan helps a newly appointed CISO integrate into the organization by building foundational knowledge, aligning strategies, and executing critical security measures across four distinct phases.

Phase 1
Pre-start preparation

Before your first day at the office.

Phase 2
Learning and Understanding

The first 30 days.

Phase 3
Planning and Alignment

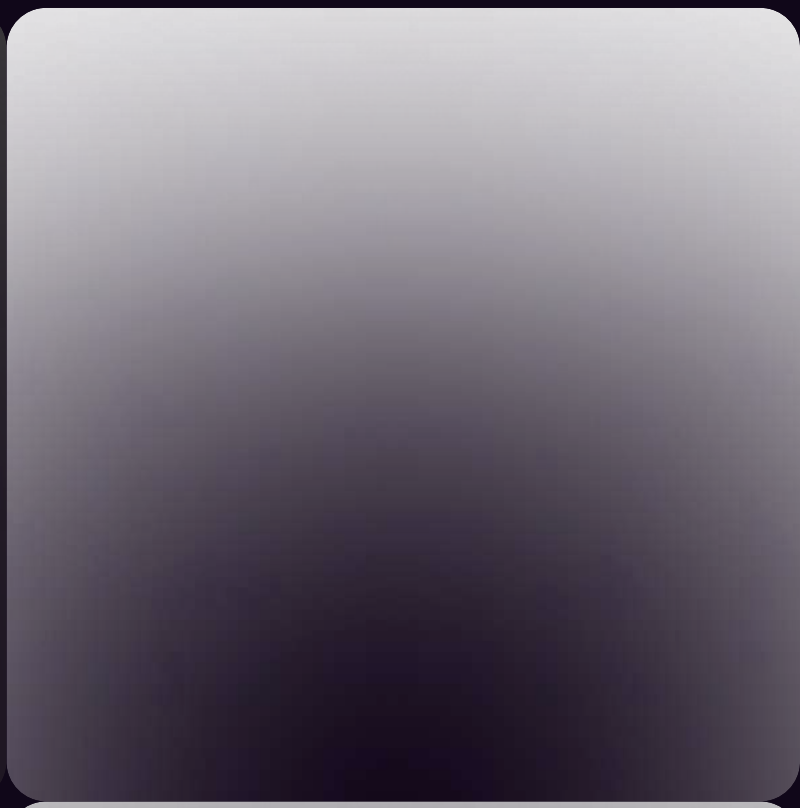
The next 30 days.

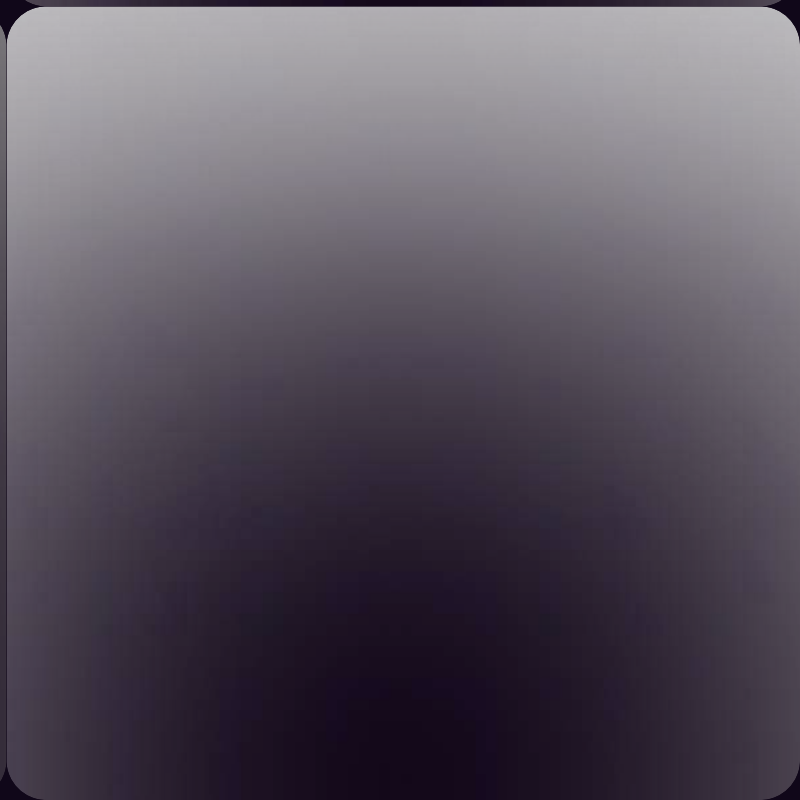
Phase 4
Execution and Feedback

The final 30 days.

Phase 1
Pre-start preparation

Understand the role, assess the maturity,
and prepare strategically with the information available.



Core objective

In this phase, CISOs in a new organization should focus on understanding the organization's role, expectations, and security maturity. This involves researching the company's history, culture, and industry-specific security challenges to prepare for the upcoming challenges and opportunities.

A CISO can use publicly available information, stakeholder engagement, and initial meetings with the security team to gauge the organization's security posture and maturity level. This helps understand specific problems the organization currently faces, as well as identify gaps and areas that need improvement.

By the end of this phase, the CISO should have a clear understanding of:

1

Stakeholder goals

Engage with key stakeholders to understand their expectations and strategic goals. This will help the CISO align security initiatives with the broader business objectives from the outset.

2

Team pain points

Based on your initial interaction with the security team, identify the challenges and concerns of the existing security team. Understanding their pain points will enable you to address immediate issues and build trust with the team early on.

3

Customer and regulatory needs

Learn about the needs and expectations of end customers and regulators. This will inform the CISO's approach to compliance and customer-centric security measures.

Practical difficulties

Limited access to internal systems

Before officially joining, a CISO will likely have limited access to company systems and internal data.

Leverage public information

Use publicly available data, such as financial reports and industry news, to gather insights about the company.

Overcoming difficulties

Understanding culture remotely

Grasping the company culture and dynamics from the outside can be challenging.

Engage with stakeholders

Schedule introductory interviews with key executives to discuss their expectations and understand the strategic direction.

The CISO Superpower

Find answers to these questions that give you a clear idea on:

Security Posture

- What are the current security measures in place?
- What are the main security risks and threats the organization faces?
- Have there been any recent security incidents or breaches?
- How is the organization's security posture evaluated and measured?

Team pain points

- Are there any gaps in the current security processes or tools?
- How does the team handle incident response and management?
- What are the major challenges in the process?
- What feedback or concerns have been raised by other departments regarding security?

Customer and regulatory needs

- What are your top priorities and concerns regarding security?
- Are there any upcoming projects or business initiatives that could impact security?
- How do you see the role of security impacting the organization's overall strategy?
- What are your expectations from the CISO in terms of security improvements or changes?

Phase 2
Learning and Understanding

Building on the qualitative work done in Phase 1, CISO should build a quantitative picture of the organization. Understanding the strategic needs of the organization and operational security issues by analyzing the company's systems and processes. Deepen the understanding of the firm's maturity and seek to establish a benchmark of current security.

Core objective

The first 30 days should prioritize building a comprehensive understanding of the company's IT systems, team dynamics, and cultural insights. The goal is to accelerate learning about the organization's systems and processes to deepen the CISO's understanding of the maturity of the security systems and processes through:

1 **Understand the digital landscape**

Ensure all assets are accounted for to understand what the security team needs to defend. This includes identifying any hidden, misconfigured, or vulnerable assets that could pose a risk to the organization.

2 **Process evaluation**

Assess existing security processes to determine if they are resource-intensive, slow, or ineffective. Understanding these processes will help the CISO identify inefficiencies and areas for improvement.

3 **Gap analysis**

Conduct a thorough gap analysis to understand where the organization's security posture is weakest. This analysis will inform the CISO's immediate and long-term priorities.

The CISO should have a "single source of truth" - a platform that gives a detailed asset inventory to assess vulnerabilities. This will help the CISO gain and maintain a clear and unambiguous image/understanding of what they are trying to protect, what is vulnerable and how good existing security processes are.

The CISO should have better visibility – the comprehensive understanding and awareness of the organization's security posture, including the status of assets, threats, vulnerabilities, and security controls across the enterprise – at this stage compared to when they came in.

Additionally, gathering feedback from stakeholders on security practices can help identify inefficiencies and areas ripe for automation. Tasks such as asset discovery and risk validation are critical for setting performance goals. Benchmarking against industry standards, such as Mean Time to Response (MTTR), will also provide valuable insights, allowing the CISO to compare the organization's performance with peers and set realistic, competitive targets.

Personal goals at this stage include meeting key personnel and establishing regular meetings with critical partners, helping the CISO to integrate quickly into the organizational fabric.

Practical difficulties

Information overload

The sheer volume of new information can be overwhelming.

Team resistance

New leadership may face resistance from existing team members.

Limited visibility

The security team might not have visibility of all the projects and technologies used by the business (e.g. new cloud deployments, IoT/OT, shadow IT, etc.)

Overcoming difficulties

Establish a “single source of truth”

Begin by creating a unified, comprehensive view of the organization's security posture, ensuring that the entire team works from the same accurate, up-to-date information. This shared understanding is crucial for the team to accurately identify priorities and focus on the most critical systems and processes.

Structured learning approach

Once a single source of truth is established, concentrate on the most critical systems and processes first to prevent information overload.

Build trust with the team

Engage openly with the team to understand their challenges, gain their trust, and foster a collaborative environment.

The CISO Superpower

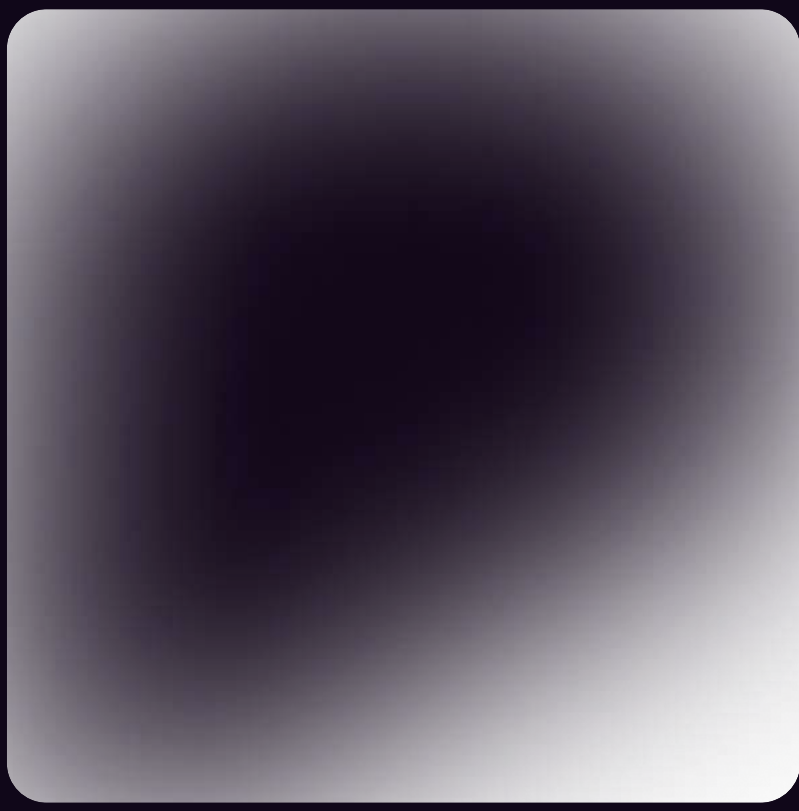
Continuous visibility and benchmarking

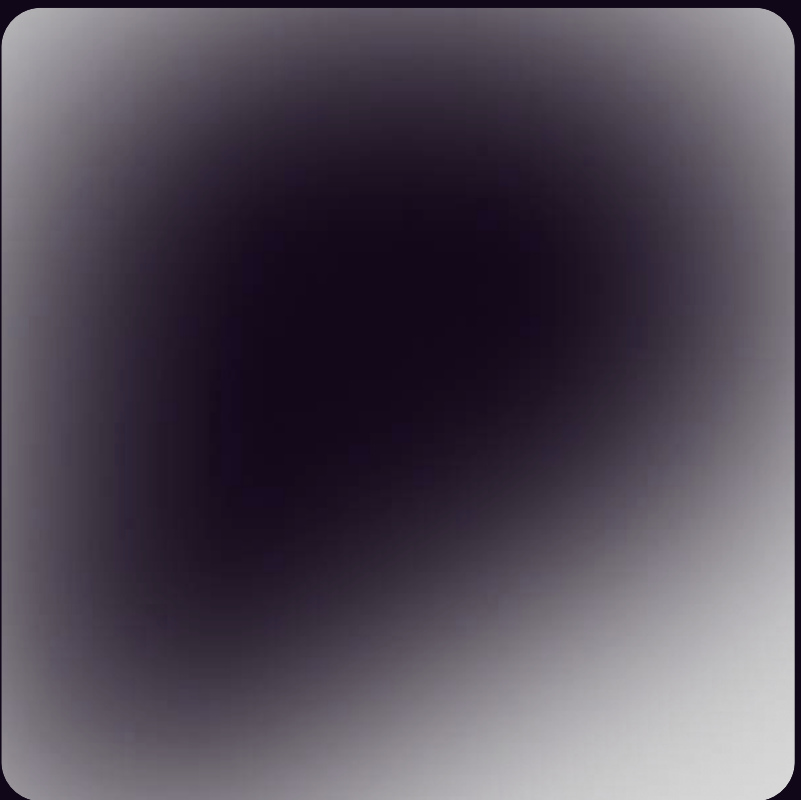
Building a thorough understanding of the organization begins with gaining complete visibility of the digital footprint. This visibility is essential because you can’t protect what you can’t see. If they are not present, CISOs should implement dynamic asset discovery tools to ensure that no part of the attack surface goes unmonitored.

The digital attack surface is continually expanding, with new vulnerabilities and exposed assets emerging regularly. CISOs should prioritize the use of automated tools that continuously discover and monitor assets in real-time. This can alert security teams to new exposures, changes in configurations, or suspicious activities that could indicate potential threats.

Phase 3
Planning and Alignment

Develop and align security strategies with business goals and develop a maturity roadmap.





Core objective

Based on the insights gained in the first 30 days, the CISO should use the next 30 days to develop a roadmap for enhancing security maturity. A crucial step in this stage is plugging gaps in security visibility with offensive security. The better visibility gained in Phase 2 will help them spot the gaps in the posture, channeling the efforts to those areas.

In this phase, the CISO should develop a clear roadmap to enhance security maturity by identifying and prioritizing gaps in the security posture. Implementing offensive security techniques will improve visibility, allowing for targeted improvements. Additionally, automating security processes will optimize resource allocation and accelerate operations by reducing manual tasks.

Action planning involves creating a security roadmap and ensuring stakeholder alignment. The CISO should integrate threat intelligence into operations and conduct operational drills, achieving quick wins and gathering feedback to adjust strategies.

Practical difficulties

Prioritizing initiatives

Determining which security measures to prioritize can be difficult.

Aligning security with business goals

Ensuring security strategies align with broader business objectives can be challenging.

Overcoming difficulties

Automated penetration testing:

By automating the penetration testing processes it could be scaled across the entire attack surface, not just the critical assets.

Frequent communication

Regularly communicate with business leaders to ensure alignment with business goals.

The CISO Superpower

When constructing plans for the security team CISOs should do the following:

1

Data-driven decision making

Use data from vulnerability assessments and penetration tests to inform priority setting. This would also rationalize the additional budget and changes in the existing processes.

2

Gap analysis and prioritizing risks

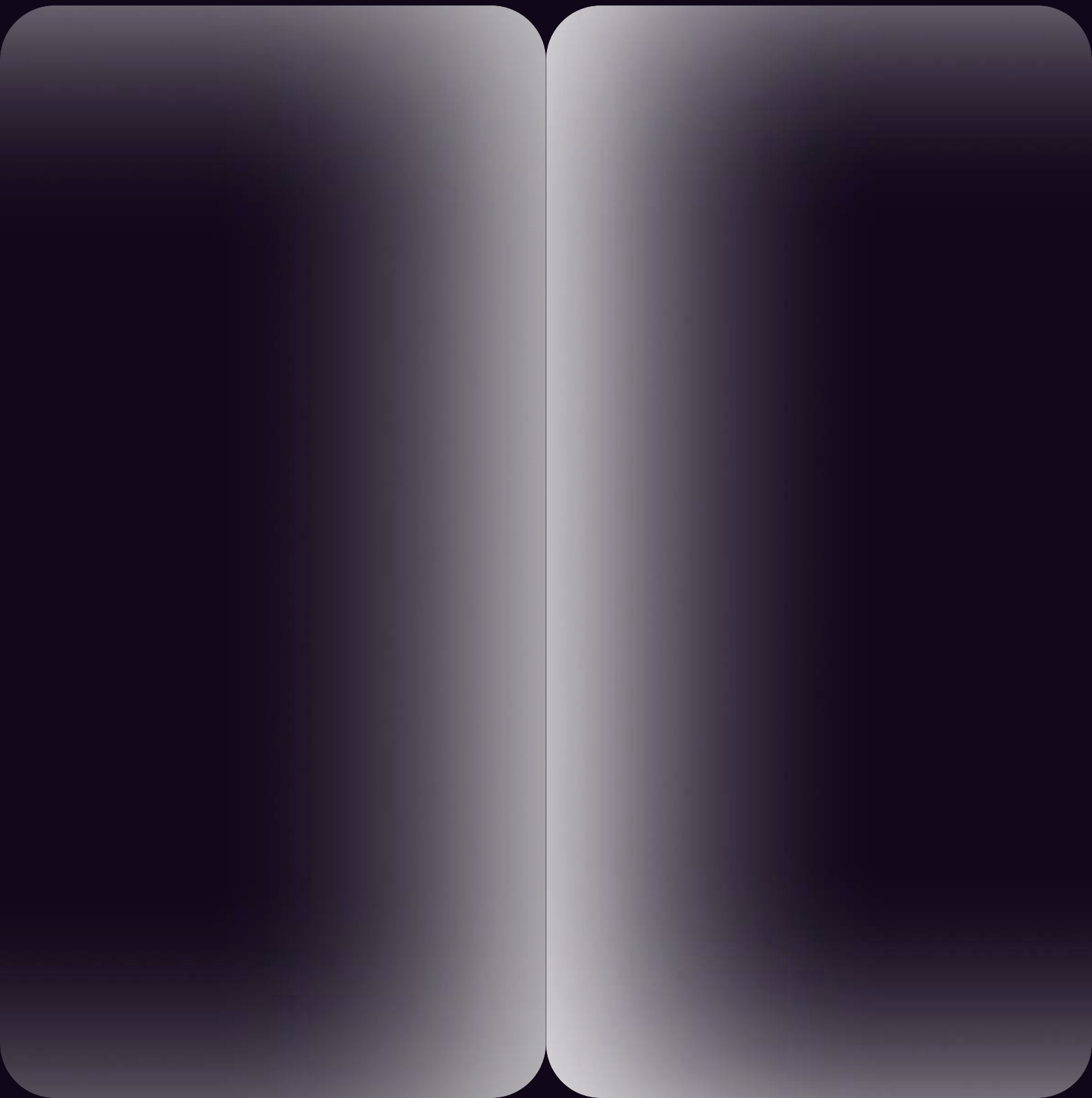
It helps in developing a maturity roadmap aligned with strategic goals for real-time threat detection.

To make data-driven decisions and effectively prioritize the team's efforts CISOs need a thorough understanding of the organization's exposure. Historically, the only way to gain this has been through penetration tests which are not scalable across the entire attack surface and are conducted infrequently. By automating penetration testing CISOs can ensure that the organization remains aware of vulnerabilities.

Automated penetration testing simulates potential cyberattacks across the attack surface, identifying vulnerabilities before they can be exploited. With continuous insights, security teams can promptly respond to newly identified vulnerabilities.

Phase 4
Execution and Feedback

Implement and consolidate security measures,
improve maturity, and demonstrate progress.



Core objective

In the last 30 days of the plan, the primary objective is to solidify the organization's security maturity by implementing and refining security measures and processes. The CISO should focus on enhancing threat management capabilities and reinforcing compliance by executing strategic security initiatives and closely monitoring progress against key performance indicators (KPIs).

As new processes are implemented and active vulnerability scanning is conducted, the CISO should leverage threat intelligence, business context, and other relevant factors to prioritize actions effectively. Automated regression testing should be used to confirm that vulnerabilities are being addressed, allowing the CISO to track improvements in the security posture. By the end of this period, the goal is to demonstrate a measurable enhancement in security posture and alignment with the organization’s strategic objectives.

Key learning goals for this phase include implementing comprehensive security awareness training and conducting professional development activities to build the team’s skills. Performance goals should focus on leading and completing new security projects, while personal goals emphasize involvement in extracurricular activities that contribute to professional growth. Regular reporting and ongoing stakeholder engagement are critical to showcasing security advancements and aligning with the organization’s overarching goals.

Practical difficulties

Sustaining momentum

Maintaining the pace of change and improvement can be challenging.

Measuring impact

Demonstrating tangible progress within 90 days can be difficult.

Overcoming difficulties

Celebrate milestones

Recognize and celebrate achievements to maintain momentum and motivation.

Use metrics for impact

Collect and present data to highlight progress and areas of improvement.

The CISO Superpower

CISOs should aim to provide quantifiable evidence that their initiatives are delivering results. They can utilize the automated asset discovery and penetration testing tools deployed in earlier phases to continuously discover and monitor assets to demonstrate progress. With these tools, CISOs can show progress in a number of ways:

1. Fewer number of risks over time
2. Reduced time to remediation
3. Improved posture of individual assets

These figures can demonstrate that a CISO has had an immediate and tangible positive impact in their first 90 days. This will simultaneously increase stakeholder and security team confidence in their abilities.

If the improvement to any of the statistics has been below expectations CISOs can use this to drive further the next 90 days of initiatives. This could include demonstrating that the security team needs additional budget or headcount to reach the desired security level.

These statistics can form the basis of ongoing stakeholder management and strategic planning for the security function.

Applicability and adaptation

This 90-day transition plan is designed to be a general framework that can be adapted for CISOs across various industries. While the plan provides a structured approach applicable to many contexts, its applicability can vary depending on several factors specific to each industry:

A

Regulatory requirements

Industries have varying regulatory requirements that can significantly impact the priorities and actions of a CISO. For example, healthcare organizations in the US must adhere to HIPAA, while in the financial industry, regulations like PCI-DSS and Sarbanes-Oxley are priorities.

B

Industry-specific threats

The threat landscape can differ widely between industries. For instance, CISOs in the energy sector might focus on protecting critical infrastructure from nation-state actors, while those in e-commerce must prioritize fraud prevention and customer data protection.

C

Technology environment

The technology stack and reliance on specific types of IT infrastructure can vary. Industries with significant IoT integration, such as manufacturing or healthcare, will require a greater focus on IoT and OT visibility.

D

Organizational culture and structure

The size and structure of the organization, as well as its culture towards security, can affect the CISO's approach. A CISO in a startup might have more agility but fewer resources compared to one in a large enterprise.

E

The Maturity factor

The existing maturity level of the security program will influence which areas need more immediate attention. A mature program might focus more on fine-tuning and optimization, whereas a developing program might need foundational improvements. The 90-day plan factors the maturity level of the security program in each phase of execution.

Applicability and adaptation

The successful implementation of this 90-day plan relies on its customization, ensuring that the plan is relevant and effective in addressing the organization's unique security concerns and compliance requirements. As your trusted cybersecurity partner, Hadrian's proprietary AI-powered platform helps you get the process right.

Hadrian's Continuous Asset Discovery and Automated Penetration Testing during the planning phase (days 31-60) helps identify weak points in your defenses. As you move into the final phase, automating Compliance Reporting streamlines the regulatory adherence process.

Prioritizing these processes will help you make the most impact in your first 90 days.

About Hadrian

Proactively mitigate threats by embracing the hacker's perspective. Hadrian reveals exploitable vulnerabilities by continuously assessing threats across your entire business with the precision of a world-class team of penetration testers. Embrace offensive security and remediate your critical exposures with less effort and cost.

Recognised by leading analysts

Hadrian is only vendor recognized as both a Leader and Outperformer in the 2024 GigaOm Radar Report for Attack Surface Management. Learn more at hadrian.io/gigaom.

"Hadrian's strengths are manifold, with its active assessment of vulnerabilities being a key highlight, thanks to its sophisticated Orchestrator AI."

Chris Ray, Analyst at GigaOm

Trusted worldwide by market leaders

CRÉDIT AGRICOLE	SHV ENERGY	amadeus
RITUALS...	LEROY MERLIN	macmillan education
ABN·AMRO	London Business School	LOTTOMatica