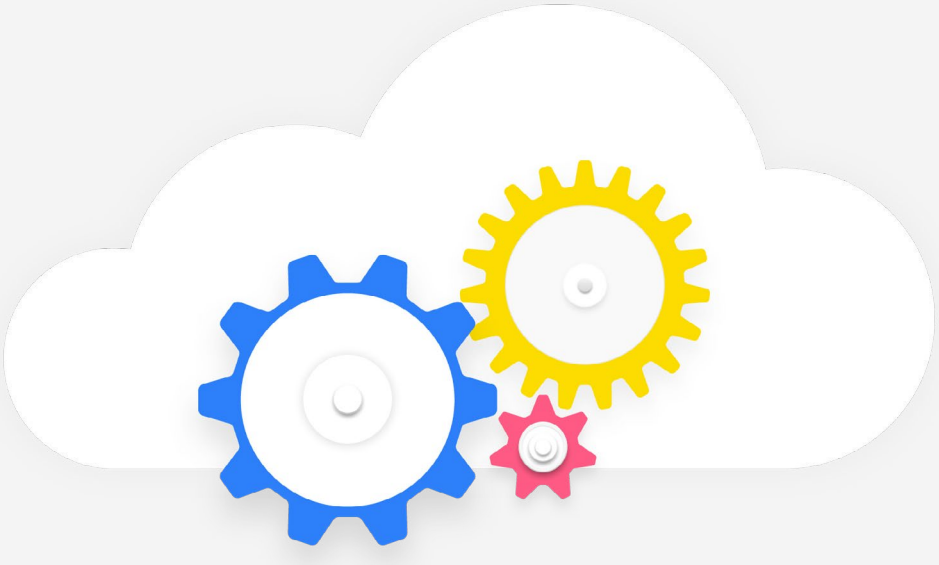
Digital-First SecOps: The Key to Cybersecurity Success in a Digital World



torq

Contents

1

Introduction

Software is eating the world. Digital transformation is the order of the day. Every business is a software business.

Axioms like these are often tossed around to highlight how businesses in general have embraced digital technology to increase the speed and efficiency of their operations over the past decade. From engineering teams, to HR departments, to marketing teams and beyond, all aspects of the typical business now take a digital-first approach to their day-to-day work. Operations that were once manual, analog, and individualized are today automated and collaborative, thanks to a new generation of digital tools.

2

A Digital-First Approach to SecOps

But what about security teams? Where do they fit into the digital transformation conversation? That's a topic often overlooked when discussing what digitalization means for modern businesses.

It's time to change that by applying the same digital transformation strategies to security teams that we've deployed for other business units. If businesses hope to cope with all of the security threats that go hand-in-hand with new digital technology, security teams need to be brought under the digital transformation umbrella, too. After all, companies can't actually solve the security and compliance challenges that they face in a fast-moving digitized world if their security teams lack the same level of automation, efficiency, and scalability that other business units enjoy.

That's why identifying and implementing digital-first security solutions is one of the major tasks facing Chief Information Security Officers, or CISOs, today. While CISOs spend much of their time assessing how risks have increased in an economy where everything – from software applications, to banking systems, to manufacturing plants, to transportation infrastructure and beyond – has been digitized and connected to the Internet, they must devote equal effort to developing solutions that can secure these digitized assets without compromising on the benefits that digitalization enables.

The solutions are out there, but they involve more than the security operations (SecOps) tools that sufficed in a past era where only some systems were digitized. To secure the modern business, CISOs need to take a digital-first approach to SecOps itself. In other words, in just the same way that businesses have digitized other functions in order to gain speed and agility, they need to overhaul their SecOps tools, teams, and culture by doubling down on digital innovation in the realm of SecOps.

What does that look like in practice? This eBook explains by discussing how to adopt a digital-first SecOps strategy. It breaks the process down into three main angles – tools, teams, and culture – and identifies what to consider within each of these domains when planning a SecOps strategy for a modern, digital-first business.

3

SecOps Challenges in a Digital-First World

Before delving into the SecOps tools, teams, and culture that enable businesses to thrive in today's digital economy, let's first expand on the reasons why the digitization of everything has made SecOps so challenging.

Digital technology is nothing new, of course. For decades, many businesses have deployed at least some software. They have also managed the application security, data privacy, and compliance risks associated with that software.

But what has changed over the past five to ten years is that virtually every system within the typical business has been digitized. The rise of the cloud, which makes software easier than ever to deploy and manage, has enabled many businesses to deploy applications in place of analog systems even if those businesses lack large in-house IT infrastructures or teams. At the same time, the rise of the Internet of Things, or IoT, has made it possible to digitize systems – such as manufacturing lines or transportation networks – that, in the past, would have been very difficult to integrate with software.

In other words, whereas digital technology was once the exception, it has become the norm. Businesses of all types, and across all verticals, have gone digital-first.

That shift enables many benefits, such as greater scalability and speed. But it also amplifies the security and compliance challenges that arise from digital systems. When businesses migrate a function or system from analog technology to a digital solution, they face a host of new compliance rules that apply only to digital technologies. They must also manage a whole new set of possible vectors for attack and abuse via software vulnerabilities, improper access controls, accidental digital data loss, and so on.

At the same time, the sheer scale on which modern digital systems operate has introduced novel risks. One of the main goals of digitalization is to allow businesses to continue to move faster at a larger scale. But the faster they implement changes, and the larger the scale on which they operate, the more quickly risks will arise. Digital transformation success, then, hinges on businesses' ability to manage risks on a much larger, faster-paced scale.

All of the above means that the demands placed on SecOps teams have exploded in scope. Instead of having to secure and monitor just a handful of applications or a small amount of digital data (which was often hosted on-premises), today's security teams must contend with sprawling, cloud-based environments that can be configured in an endless variety of ways, and which are subject to innumerable potential security risks.

Likewise, instead of only having to manage servers and monolithic applications, modern security engineers must manage the complexities of containerized, microservices-based applications orchestrated by Kubernetes, which introduces a range of security risks of its own. And rather than overseeing assets located in the same physical facility and connected to the same secure network, security organizations today must secure teams of distributed workers who rely in part on private devices and home networks to do their work.

If you're a CISO, you are probably already intimately familiar with risks and challenges like these. You've been living in a digital-centric world for at least several years, and you're aware that your business faces a variety of digital security threats that simply didn't exist five or ten years ago, back before the business went all-in on digital technology.

4

A Digital Approach to SecOps: Tools, Teams, and Culture

What you really want to know as a CISO today is how to manage the security risks that exist in a digital-first business. The answer is digital-first SecOps.

To understand what digital-first SecOps looks like in practice, let's discuss the concept from the perspective of tools, teams, and culture.

Tools

Modern SecOps tools haven't changed fundamentally over the past decade. They still operate on the premise that teams need to identify, assess, and remediate security risks based on anomalies within the digital systems they manage.

What has changed from the perspective of SecOps tools, however, is the extent to which they need to enable proactive and collaborative response to threats.

In the past, it may have sufficed to deploy security tools that monitored production systems and generated alerts when something looked awry. But today's SecOps tools need to be able to detect threats proactively based not just on data collected from software environments, but also from threat intelligence research, vulnerability databases, configuration audits, and the like. With this information, SecOps tools can alert teams to many risks before the risks escalate into active threats.

At the same time, modern SecOps tools need to drive collaboration. Today's SecOps teams don't exist in a silo. For businesses that continuously update the software applications on which they rely, SecOps teams must work closely with developers, IT engineers, and other stakeholders to ensure that everyone has visibility into security risks – and that everyone is prepared to collaborate efficiently in fixing those issues.

To achieve both of these goals – proactive response and collaboration – security automation is key. SecOps teams can't hope to detect risks proactively, or work efficiently with other stakeholders to address them, if they attempt to manage risks by hand. There are too many potential threats, and too many digital assets that the threats could impact, for a manual approach to work.

Equally important is choosing tools that enable seamless collaboration by all stakeholders – including but not limited to SecOps teams – around security issues. Expecting security teams to protect the whole business from within their silo is no longer enough. The business needs security tools that everyone can access and employ to drive a security culture grounded in collective responsibility.

To sum up, then, SecOps tools for a digital-first world need to deliver automation that allows SecOps teams to detect threats proactively, while also providing the collaboration features and ease of use necessary to loop in other stakeholders. Automation, collaboration, and ease-of-use are what separate digital-first SecOps tools from conventional SecOps tools.

Teams

In the past, you could build an effective security team by hiring engineers who were experts within certain technologies or domains.

That approach no longer works, for two reasons. One is that, in the digital age, security threats are increasing in scale much faster than teams can grow. As a result, security teams need to find ways to operate more efficiently, and to do more with limited human resources.

The second challenge is that security threats change so quickly in type and form that it's no longer realistic to rely on a team of experts who specialize in one type of protection. CISOs must instead focus on building security teams who are prepared to respond to any type of risk – even those that they don't foresee.

CISOs can address both of these challenges by constructing collaborative teams. When your security team can collaborate seamlessly with other parts of the business, it becomes much easier to address the challenges associated with the ever-increasing scale of modern security threats. Security engineers who can collaborate closely with the employees who actually use the technologies that the security team secures can lean on the business as a whole to increase their operational capacity. Security teams that specialize in certain tools or technologies can't leverage the business to scale their operational capabilities in this way.

Likewise, collaborative teams enjoy the ability to work alongside technology experts when they need to learn a new tool or master a new type of threat. In this regard, collaborative security teams are best positioned to remain effective in a world where new types of security threats are emerging constantly, and new tools are becoming available to detect and remediate them. In other words, collaborative teams are always ready to learn new tricks – a key attribute for a digital business.

Culture

Ultimately, a business's security operations are only as effective as its security culture. That's especially true for digital-first businesses that face security risks around every corner, and in which threat actors may use methods (like phishing) that target employees for whom SecOps is not an official job responsibility.

The question for CISOs, then, is how to embed a cyber security culture across the business and instill cyber resilience into the company's DNA.

Security automation that every employee can access and help to implement also plays a key role in achieving this goal. When you transform security from something that only credentialed SecOps experts can handle into a task that each of their co-workers can also "own" through no-code automation, it becomes much easier for a security culture to permeate the business.

What's more, the ability to democratize security using easy-to-access, collaborative security automation tools makes it easier to recognize and celebrate the contributions that all employees make toward security. Historically, security has been a thankless job; security teams only came under the spotlight when something went wrong, and their success in preventing threats was harder to measure or highlight.

But when security becomes part of everyone's day-to-day routine, and when contributions to security can be measured through efforts to deploy security automation tools, CISOs are in a position to transform security into an aspect of company culture that everyone appreciates and celebrates. Success can be measured in terms other than how many breaches take place in a year, and credit for security efforts can go to employees of all types, not just the security team narrowly defined.

5

Conclusion: SecOps for a Digital World

Instead of worrying about the new challenges that your business faces in a digital-first world, address the challenges by adopting a digital-first approach to SecOps. Digital-first SecOps means applying the same level of automation, speed, and business-wide accessibility for security that digitization has brought to other aspects of the business.

Torq can help. Through no-code security automation, Torq modernizes how security and operations teams work with easy workflow building, limitless integrations, and numerous prebuilt templates. It turns SecOps from a slow, manual affair into an IT function that every stakeholder can embrace and accelerate.

Learn more by **requesting a demo**.

Torq is a no-code automation and orchestration platform for security and operations. We empower frontline security teams in their journey to becoming more efficient by allowing them to automate processes using our easy workflow builder, limitless integrations, and numerous prebuilt templates.

Built as an enterprise-grade software-as-a-service, Torq can be adopted with ease, delivering results within minutes, unlike traditional security automation solutions that require weeks or months of investment prior to providing value.