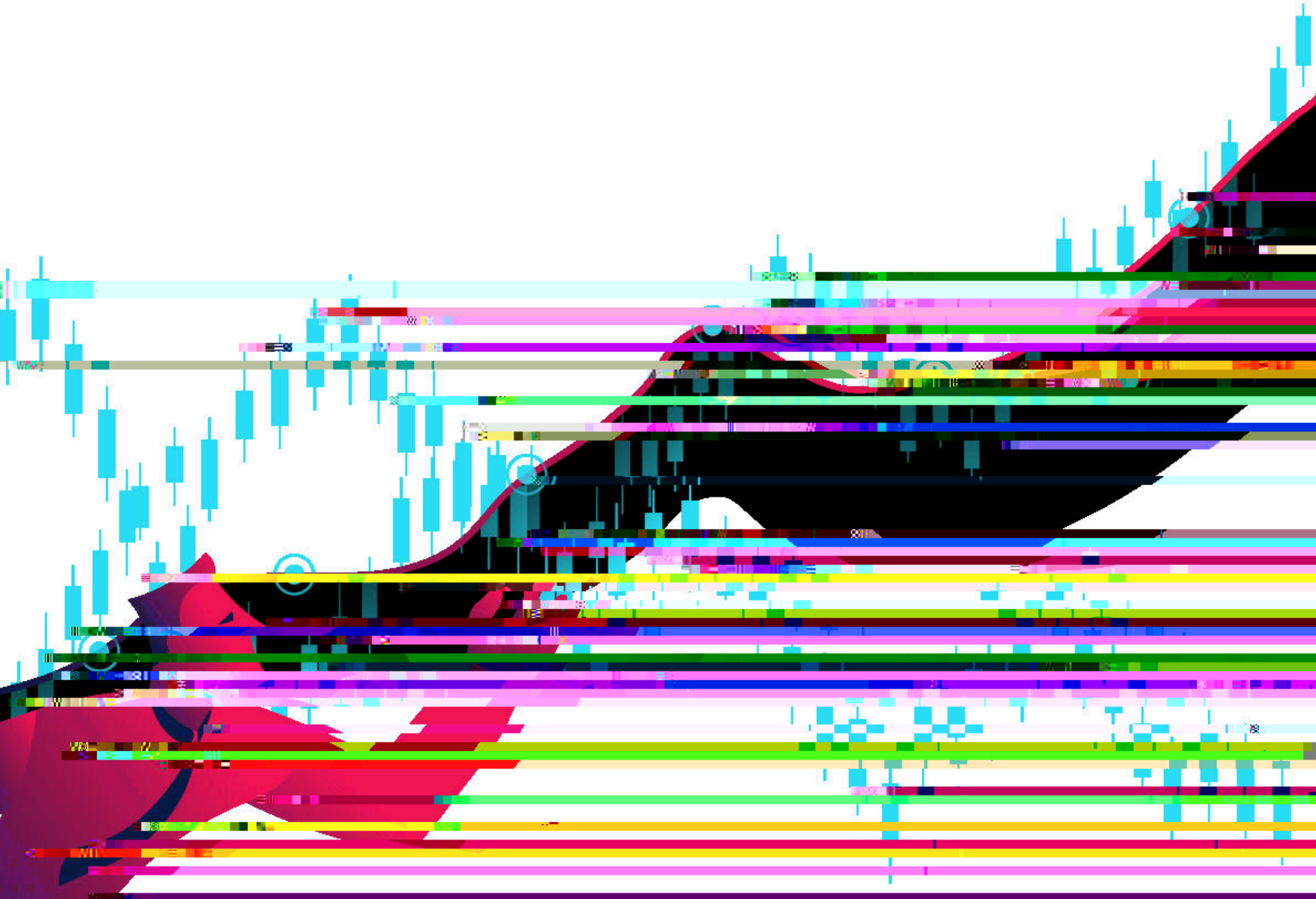
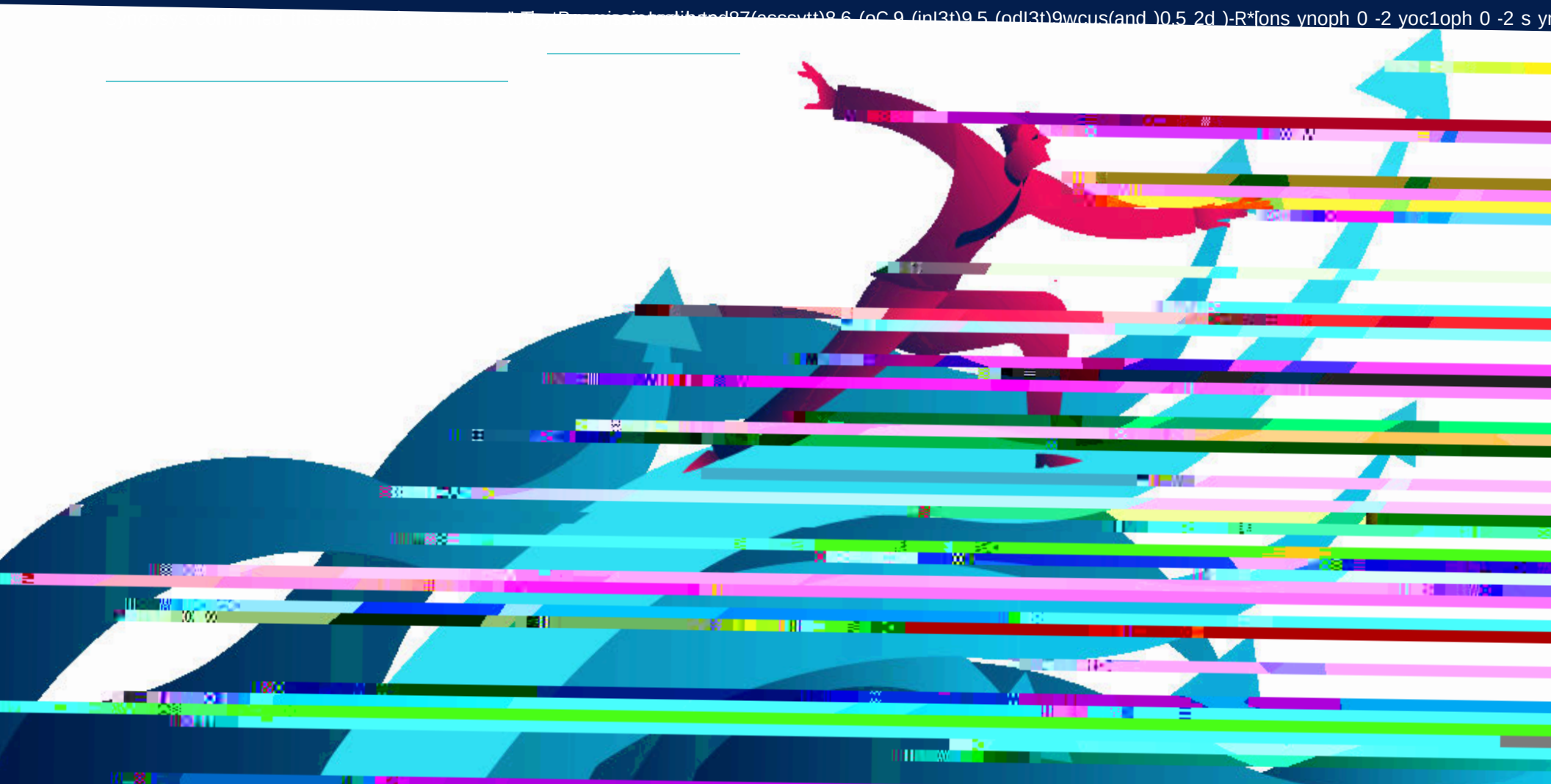
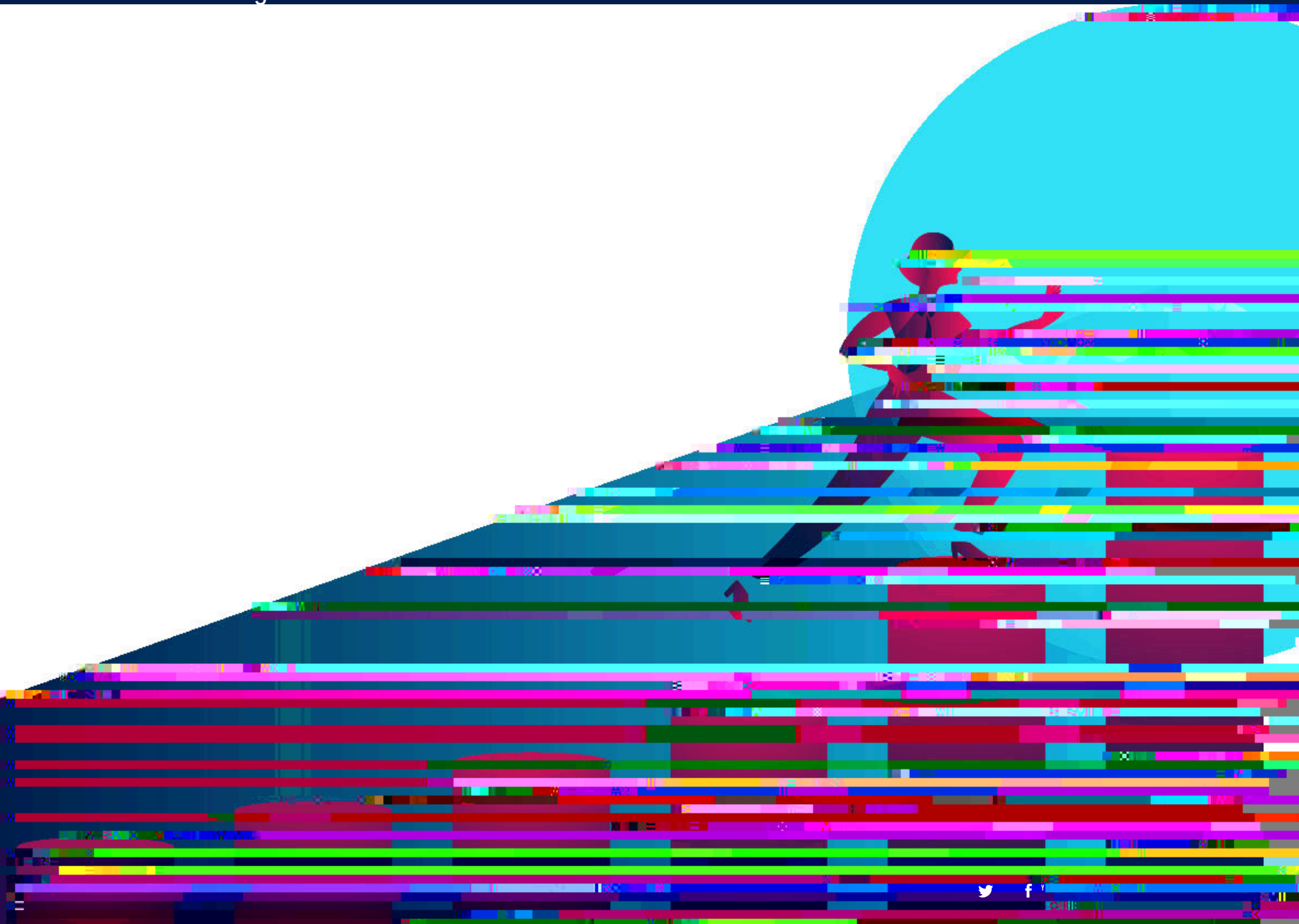
S



In the dynamic and ever-changing technology landscape, financial services industry (FSI) organizations are rushing to adopt new technologies aimed at automating internal processes, improving margins, and modernizing online and mobile experiences for customers. At the same time, these organizations must quickly transform their AppSec practices and streamline their DevSecOps strategies in response to the rapid increase in development velocity.

As FSI firms prioritize modernization efforts and adapt to competitive pressures, they struggle to implement the AppSec tools and processes critical to securing their applications at the necessary speed and scale. Misalignment between transformation and security efforts results in increased risk to both the business as a whole and to clients' sensitive data.

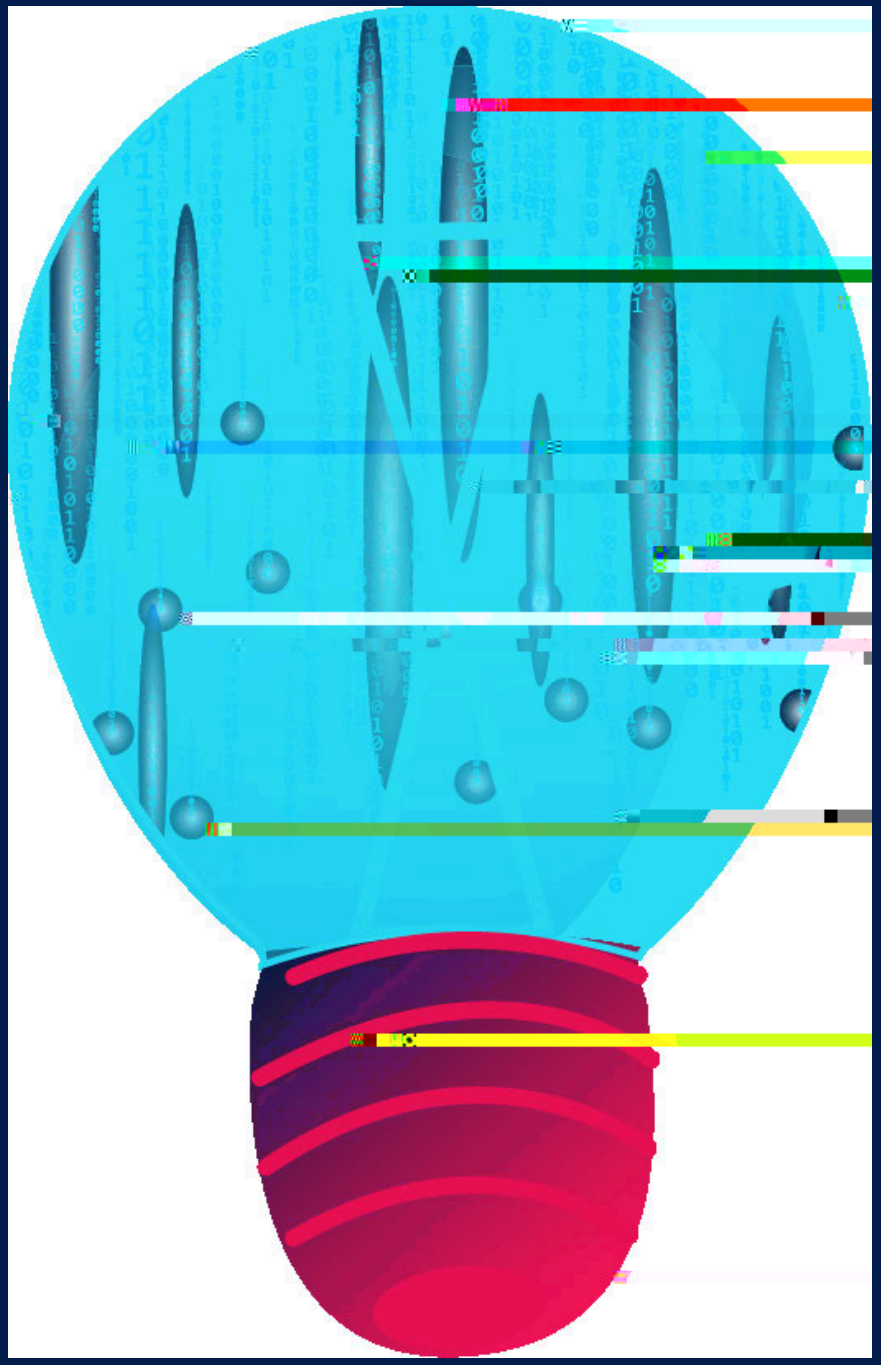




Challenge 1: Supply Chain Security

Knowing what's in the code

When tackling software supply chain security, it's important to acknowledge that there is no single conclusive method or strategy for guaranteeing absolute security. The supply chain is a massive expanse of items and factors, including who wrote the code, how they wrote it, who reviewed it,



Securing the open source your teams build with

Today, open source is everywhere. Your developers undoubtedly use open source in nearly everything they create—meaning that large portions of your applications consist of code that you didn't write. Addressing security at every single point in your supply chain is imperative, but one of the greatest threats to your overall security is the mismanagement of open source. Open source finds its way into your supply chain via two channels: from your internal developers using open source to build, and from inherited third-party software.

The "2021 Open Source Security Risk and Analysis" (OSSRA) report from Synopsys confirms this fact: 98% of the codebases scanned in the study contained open source. Of those, 84% had at least one vulnerability, with an average of 158 vulnerabilities per codebase. This data indicates that organizations are not appropriately managing open source. When inheriting code someone else wrote, you inherit its vulnerabilities, its countless transitive dependencies, and its license obligations. Without proper practices to manage this, you expose your organization to significant security risk. Unpatched vulnerabilities, whether they are a mistake or a malicious attack, can severely affect your supply chain.

Identifying and securing open source in your third-party software

In addition to using open source in your builds, your organization may rely on commercial third-party software to deliver your products and dependencies, and license obligations s well,g and(the)6.6 (ymusut)-1.1 (allber

Securing proprietary code

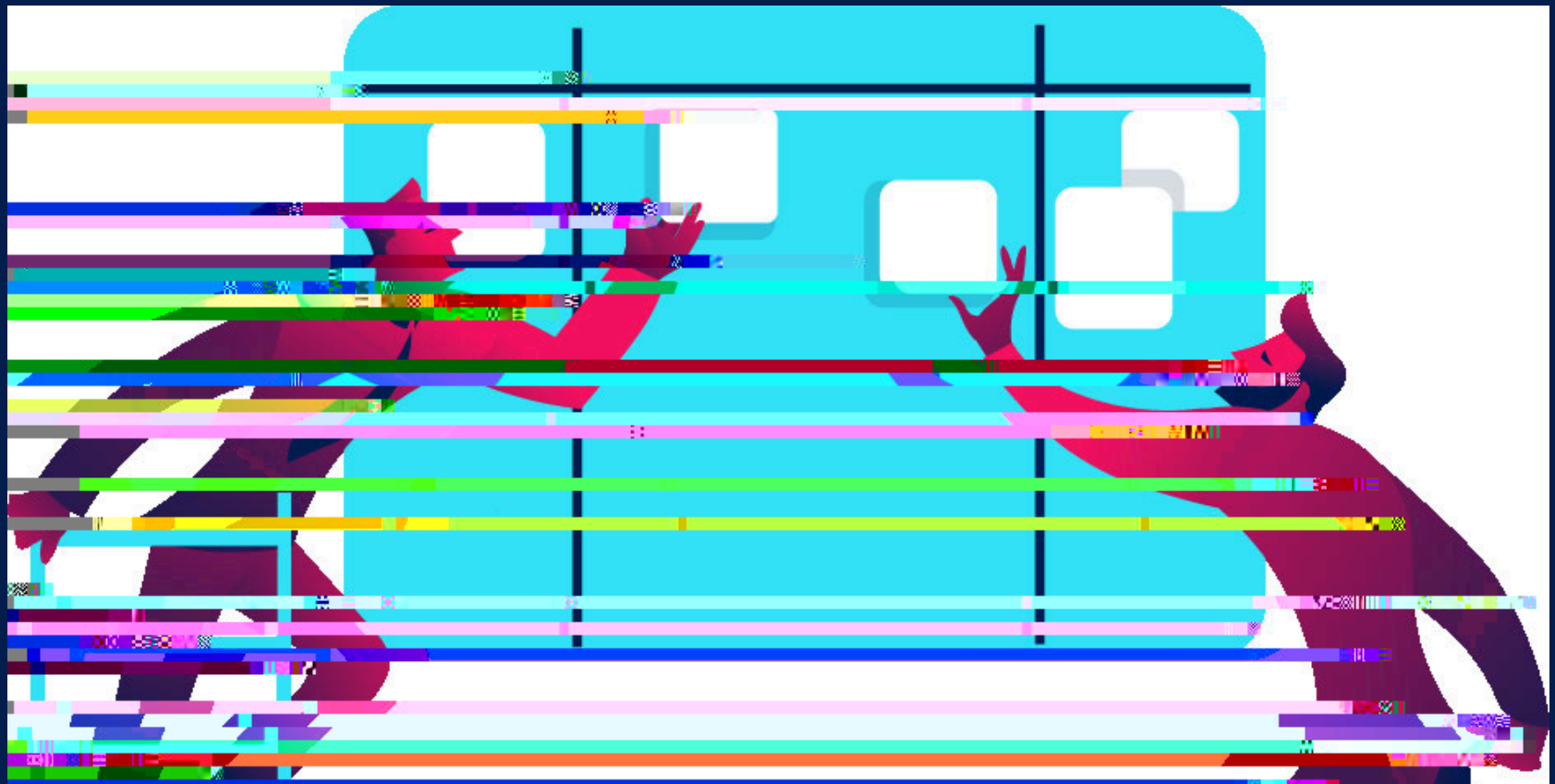
If you develop applications internally, supply chain security must be holistic and complete. Your supply chain encompasses everything from the security tools you use to the training and education of your developers. This demands comprehensive AppSec solutions; you need to manage and secure every single thing that goes on in your supply chain.

Adding a layer of difficulty, developers often lack the knowledge to practice secure coding techniques, or they haven't been trained in the best practices that are crucial to the overall health of your supply chain. And with new data privacy laws and increasing cybersecurity attacks, you need tools and solutions that prevent sensitive data leakage and ensure compliance to standards including PCI DSS, OWASP, CWE security, and more.

Organizations often must balance development velocity and security. It is crucial to incorporate solutions that let developers get started quickly and receive analysis results and remediation advice they can actually trust while they code. Without solutions capable of performing at this level, security inevitably hinders development speeds.

Facing the overarching challenge

Setting up the proper processes, policies, and tools to help effectively manage security throughout the development life cycle is a challenge. To adequately address supply chain security, you need to adopt an ongoing and constant security stance. This means you need to know about the weaknesses, vulnerabilities, and dependencies in the code, as well as the vulnerabilities in those dependencies. You also need a way to easily patch them and ensure constant monitoring. You need a clear picture of what's in your development environment, a way to manage your dependencies (maintain updates, version control, code change review), and a means for



nerabilities and offer overlapping
mportant to find all vulnerabilities
d to appropriately handle your
n all this noise? How do you know
which should be prioritized, and
e importantly, how do you know
ble threats to your development

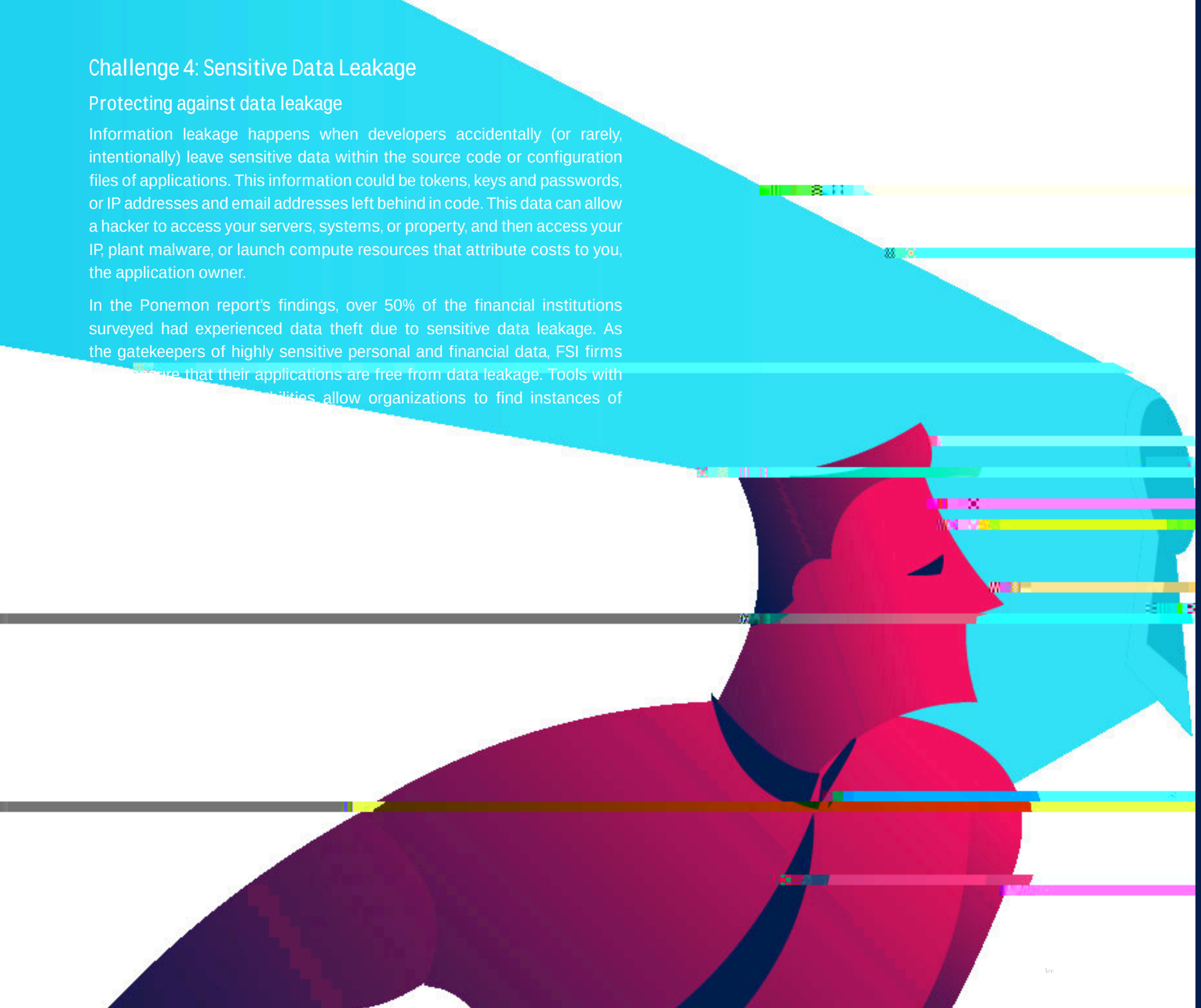
this information and synthesize it
w what you need to do and when

Challenge 4: Sensitive Data Leakage

Protecting against data leakage

Information leakage happens when developers accidentally (or rarely, intentionally) leave sensitive data within the source code or configuration files of applications. This information could be tokens, keys and passwords, or IP addresses and email addresses left behind in code. This data can allow a hacker to access your servers, systems, or property, and then access your IP, plant malware, or launch compute resources that attribute costs to you, the application owner.

In the Ponemon report's findings, over 50% of the financial institutions surveyed had experienced data theft due to sensitive data leakage. As the gatekeepers of highly sensitive personal and financial data, FSI firms [illegible]re that their applications are free from data leakage. Tools with [illegible]bilities allow organizations to find instances of



Challenge 5: DevSecOps

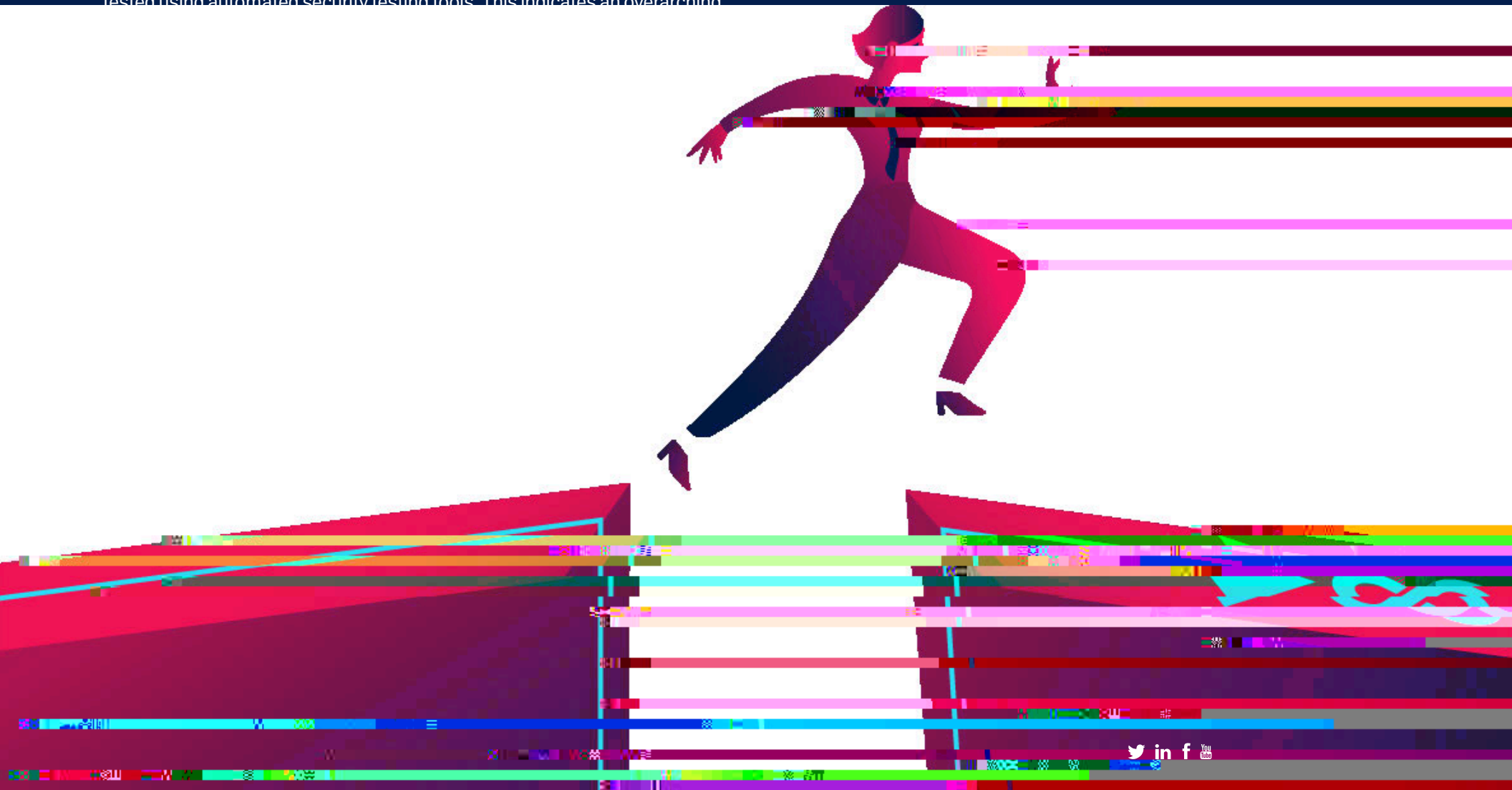
Achieving DevSecOps

If your organization develops its own applications in-house, you likely are somewhere on the journey toward adopting DevSecOps. Whether just starting or well on your way to automating and streamlining your development and security practices, achieving a successful and thriving DevSecOps environment is a never-ending effort.

Automation is a key pillar of DevSecOps and it must be central to any security initiative. The Ponemon report noted that only a third of the software produced or consumed by financial services industry organizations is tested using automated security testing tools. This indicates an overarching

The goal of DevSecOps is to bridge the gaps between teams (IT, security, development) to ensure the delivery of safe and secure code, quickly. Without tools and solutions that enable the automation necessary for this effort, an organization is likely to struggle with DevSecOps adoption.

Customers are relying more heavily on digital (mobile) offerings, and FSI firms are under great pressure to deliver new products and services that keep up with this demand. Legacy infrastructure and growing compliance and security challenges compound an already-challenging security landscape. By arming your security teams with DevSecOps solutions and tooling, you can aid in delivering superior products, faster.



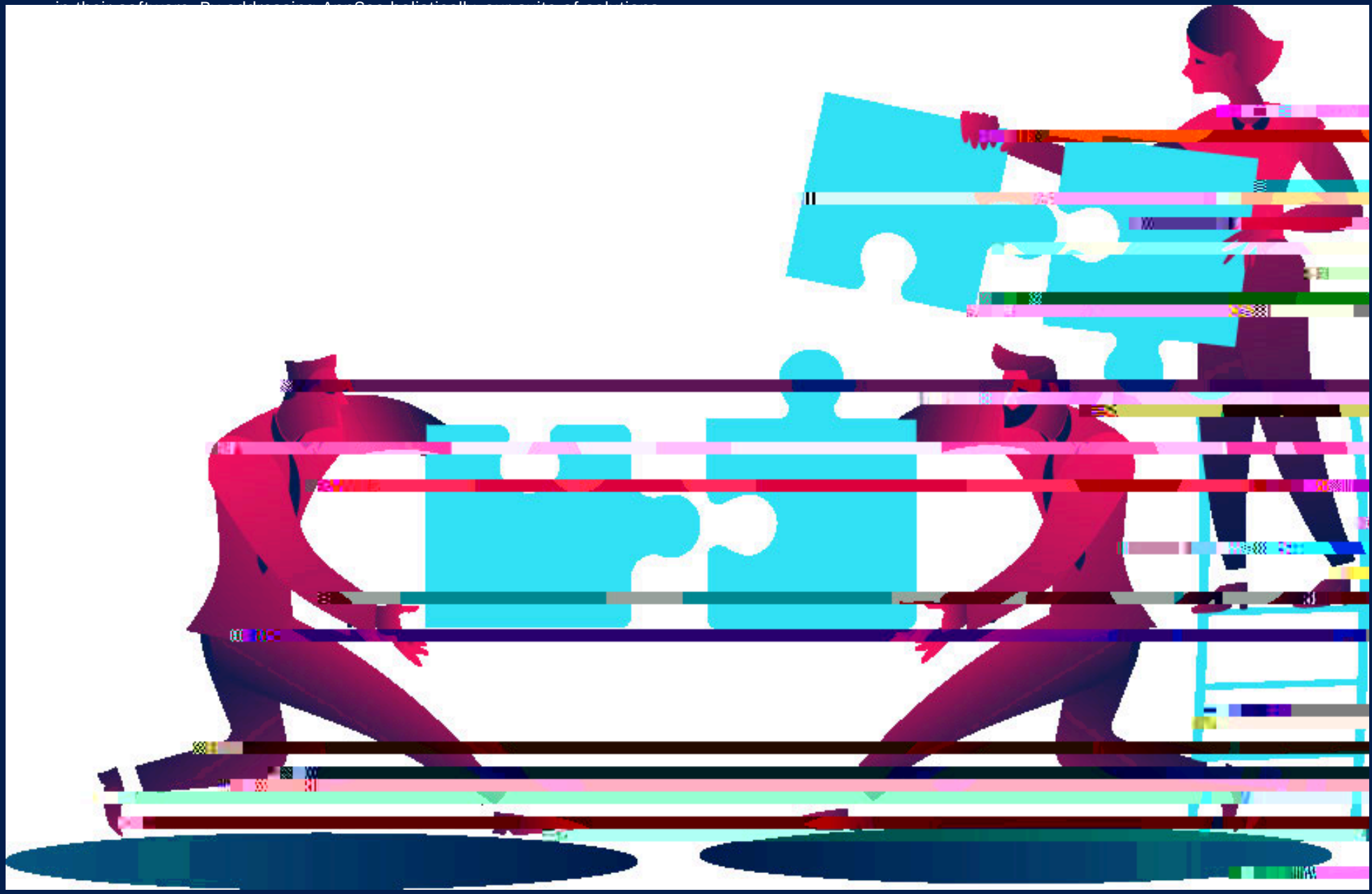
Challenge 6: Scarcity of Resources

Finding more security experts

As an FSI firm, you are in the business of serving your customers—so security training is not always the top priority. But without security experts, or at least security-aware individuals, application security becomes a major

The Synopsys Solution Suite: Modern Solutions for Modern Challenges

As a global AppSec leader, Synopsys empowers organizations to build trust



Solution 1: Black Duck and Coverity to Secure the Supply Chain

Perhaps the most important step toward securing your supply chain is knowing what's in your software.

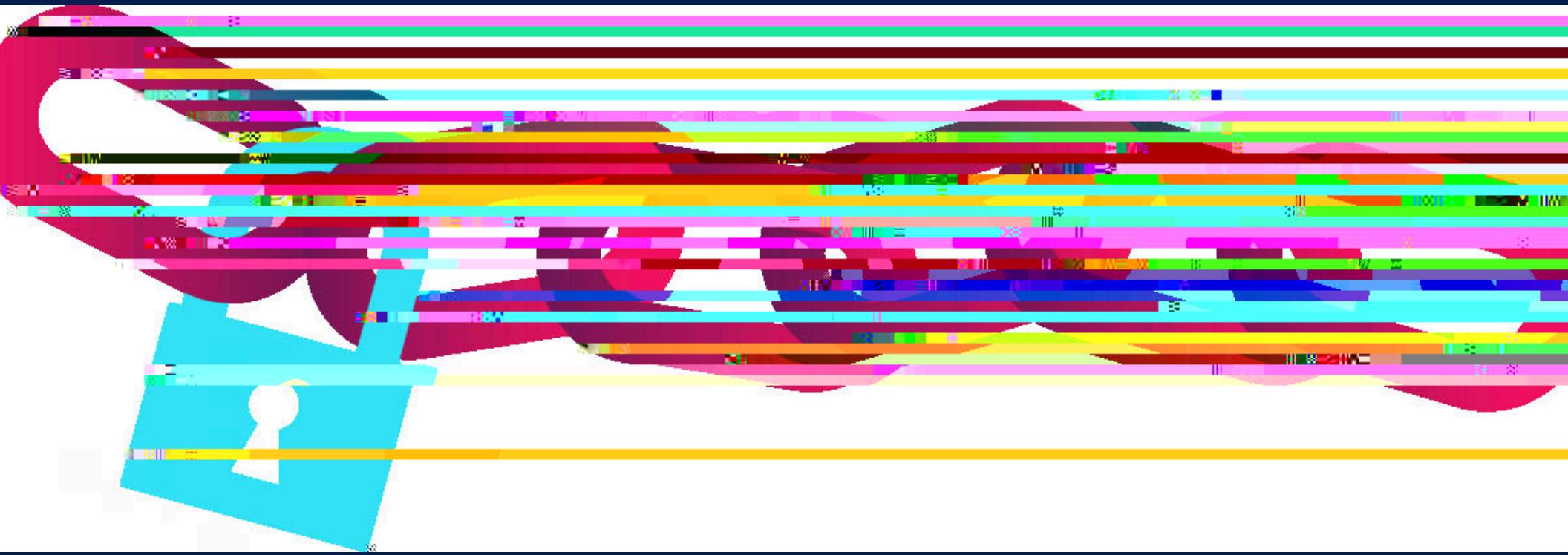
Securing the supply chain means securing all components, activities, and policies across your organization, and finding and fixing quality and security issues. The code you develop internally, the open source your developers use, and the third-party software you rely on—everything must be secured. Beyond simply securing your supply chain, you need to build trust in it: You and your customers must be able to trust the integrity of your software. No matter what your supply chain looks like, Synopsys has the solutions to secure your entire development environment and build this trust.

Securing the open source your teams use

The prevalence of open source necessitates that you view it differently. It's no longer a question of if your developers use it in your development environment, it's how much they use and how trustworthy it is. Without a complete picture of your open source, you can't protect yourself from risk.

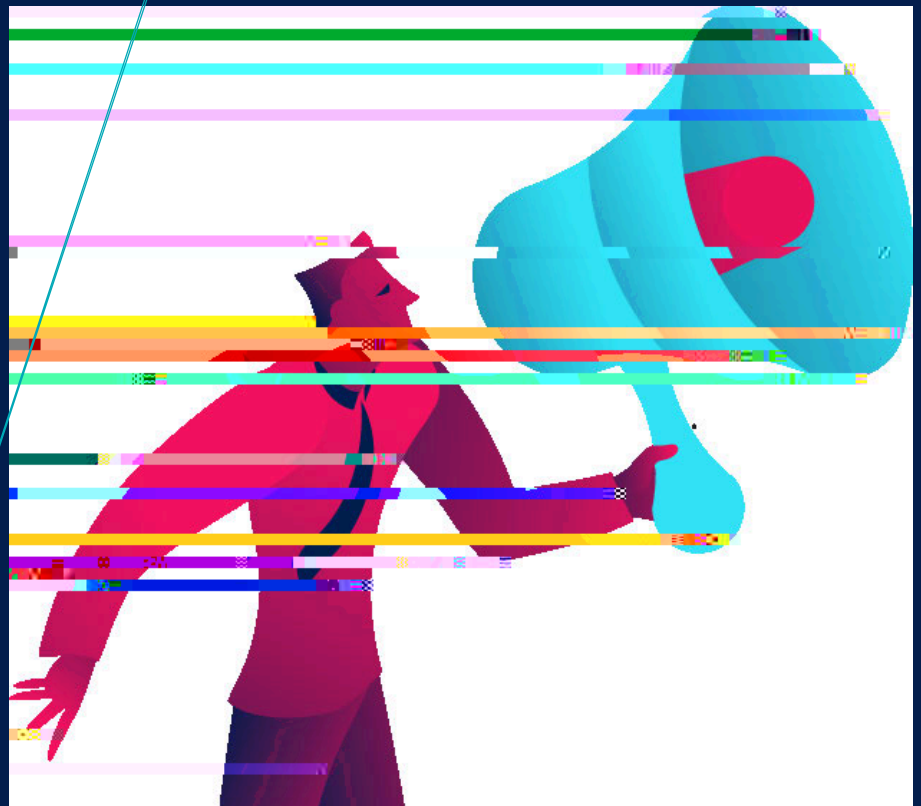
The Ponemon report found that a troubling 57% of respondents don't have an established process for inventorying it or managing the use of open source.[8] This means over half of the FSI firms surveyed don't have a proper grasp of their open source usage, its implications for their supply chain security, and the risk to their business as a whole. The need here is not simply to establish reactive policies and practices that help secure open source—it is to create a proactive security program that helps avoid future security concerns, identifies problematic components, and saves time and resources to further reduce your risk. You need a program that inspires trust in the software you're developing and provides demonstrable evidence of your trustworthiness to your customers.

Black Duck® software composition analysis (SCA) from Synopsys helps your teams manage the security, quality, and license compliance risks that stem



Black Duck's key functionalities support critical open source usage needs.

- **Black Duck helps you see into your supply chain.** Black Duck provides visibility into your software supply chain and helps you track what open source components are going into your software. With multifactor open source detection, Black Duck goes beyond relying solely on declared dependencies. This means that all open source is discovered, and a complete inventory is compiled for your developers.
- **Black Duck helps you establish trust with your customers.** Black Duck makes it easy to effectively communicate the makeup of your software to your customers and comply with emerging regulations. Black Duck also provides reports that detail what and who built your applications. It does this by exporting to Software Package Data Exchange (SPDX), an open standard for software Bills of Materials. SPDX is a recognized format as defined in the supply chain security executive order (EO 14028).
- **Black Duck gives you control over supply chain risks.** Black Duck makes it easy to proactively manage the security and quality of your supply chain. It delivers operational risk metrics like contributors, new versions, commit activity, and activity trends over time, empowering you to take action early and proactively. With Black Duck you get insight into the quality of your components and an understanding of how actively your open source is maintained.
- **Black Duck helps you stay informed when new vulnerabilities are found.** Black Duck Security Advisories provide detailed open source vulnerability records that are sourced, curated, and analyzed by the Synopsys CyRC. They deliver timely, thorough, and actionable vulnerability research directly to your Bill of Materials (BOM), so you can effectively prioritize and remediate vulnerabilities before a breach. Black Duck further ensures your open source license compliance, tracking over 2,500 open source licenses, helping you avoid license violations and protecting you from costly litigation loss of your valuable IP.
- **Black Duck helps maintain development velocity.** Black Duck enables you to set up precise and customizable policies that are automatically enforced. With multiple scan types fine-tuned for specific roles across the SDLC, you can easily enforce open source governance without slowing your developers down. Black Duck helps you align your actions and priorities with your unique risk tolerance with minimal input and action needed from your development teams.



"When we built our business case for bringing in Black Duck, our internal information security group was a cosponsor of the effort. This group now has a significantly easier way to determine which artifacts and versions are affected by any security vulnerability and which applications are impacted as a result. This

Identifying and securing open source in your third-party software

When an FSI company relies on outside providers for third-party software and then integrates this software within their own applications or through the firmware of devices embedded in their products, they open the business up to risk. The only way to truly protect your organization from this potential risk is to implement your own security practices around the treatment of third-party code and software.

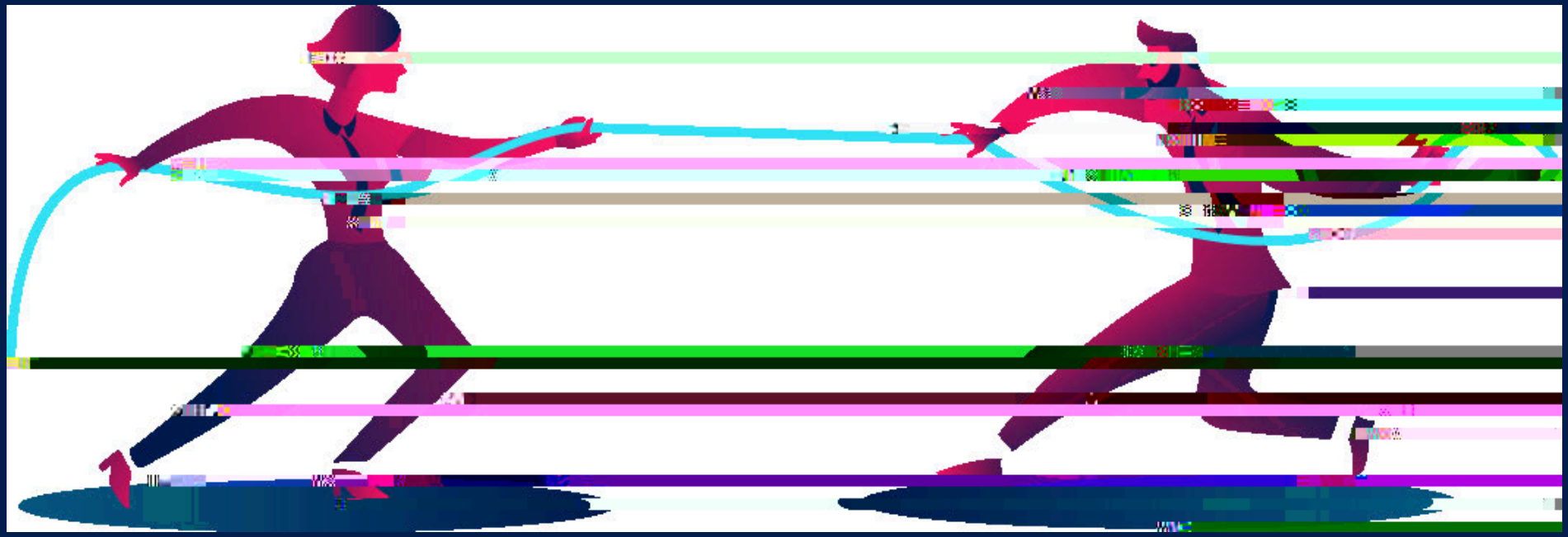
The Ponemon report found that most organizations don't have any established process for inventorying or managing their use of open source. Only 43% had any concrete process in place.[9] Black Duck Binary ABDBA

Solution 2: Code Dx for Vulnerability Overload

Code Dx® by Synopsys is an automation platform that helps you manage vulnerability overload. According to the NIST SATE V report, 66% of all AppSec findings are noise. This translates to a lot of time wasted on unnecessary and redundant triage activities.[11]

With Code Dx, you can effortlessly correlate your results, prioritize your vulnerabilities, and get a centralized view of your business risk. Code Dx's powerful capabilities include

- **Result correlation.** At its core, Code Dx is a powerful correlator. The Code Dx Correlation Engine dramatically reduces the time you spend combining and correlating the results from all your AppSec tools to eliminate redundant findings. By combining results from dynamic, commercial, and open source tooling into a single console, you can easily cut through the noise and rely on a single location to view and manage your vulnerabilities.
- **Vulnerability prioritization.** Code Dx Triage Assistant uses machine learning to intelligently predict which vulnerabilities are most critical and pose the greatest threat to your organization. Vulnerability findings are automatically prioritized based on compliance standards such as NIST, PCI, HIPAA, DISA, OWASP Top 10, and more, along with your unique business rules.
- **Centralized risk visibility.** Code Dx provides a 360-degreee view of risk for



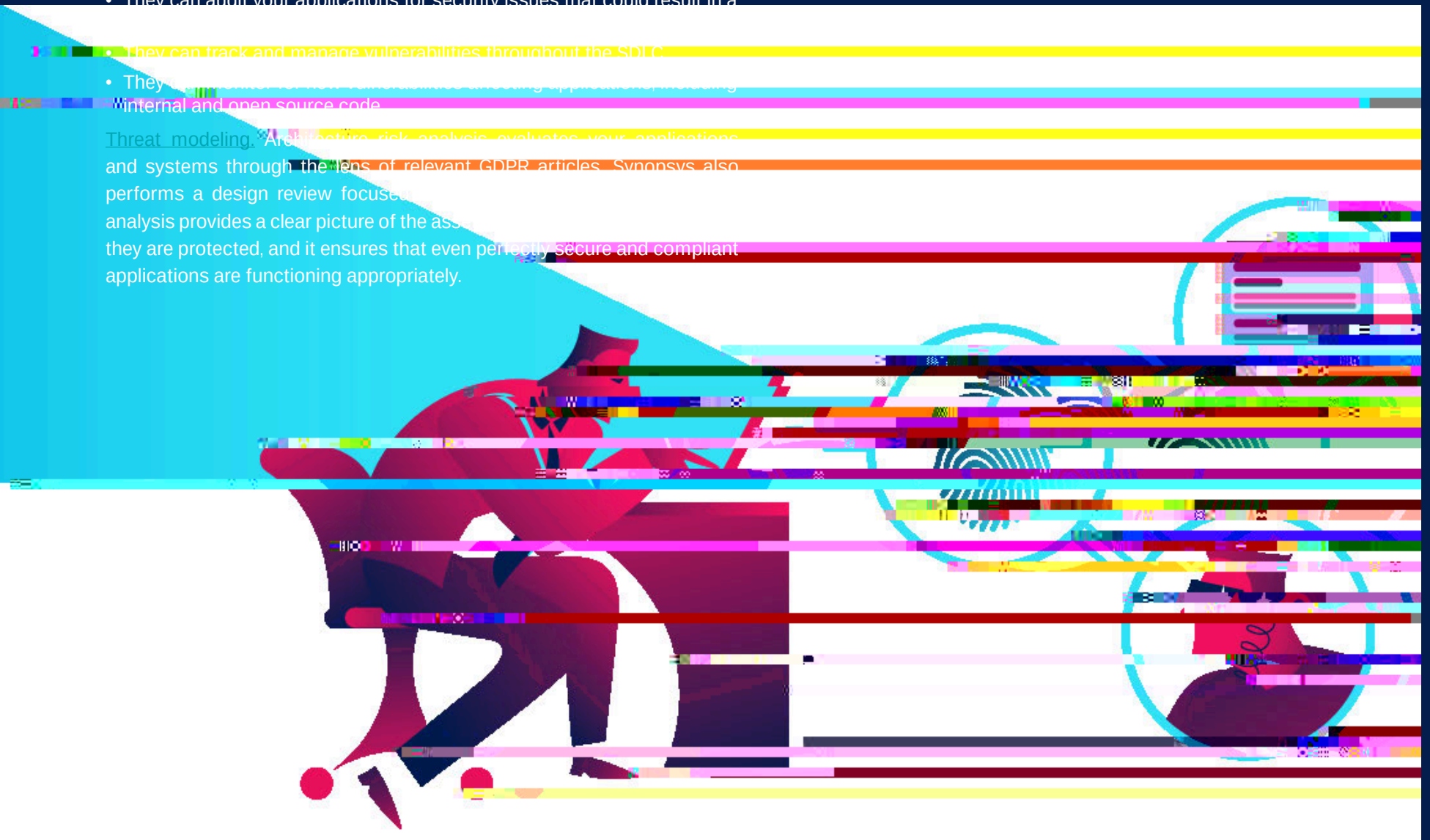
Solution 3: Synopsys for Data Privacy/Protection

Protecting data has never been more imperative for the financial services industry. Having the right tools helps you understand your risks and makes it easy to address them. Synopsys solutions help organizations eliminate attack vectors, preventing hackers from exploiting weaknesses in application security practices and gaining access to personal data. It can also help keep you compliant.

Synopsys solutions provide three key functionalities to help you avoid noncompliance.

- They can audit your applications for security issues that could result in a
- They can track and manage vulnerabilities throughout the SDLC
- They [illegible] internal and open source code

Threat modeling. Architecture risk analysis evaluates your applications and systems through the lens of relevant GDPR articles. Synopsys also performs a design review focused [illegible] analysis provides a clear picture of the ass[illegible] they are protected, and it ensures that even perfectly secure and compliant applications are functioning appropriately.



Solution 5: Code Dx, Intelligent Orchestration, Coverity, Black Duck, and Seeker to Support DevSecOps

Successful DevSecOps is a hefty undertaking and one that will not look the same across organizations. The guiding principle of DevSecOps is harmonizing development, security, and operations through the use of tools, practices, and policies that streamline the delivery of secure software, quickly. The Synopsys solution suite was designed to support this goal, automating your security efforts across the SDLC and empowering teams to tackle security confidently.

Intelligent Orchestration is a powerful tool that makes development at the speed of DevOps possible. Intelligent Orchestration allows teams to integrate AppSec analysis into their DevOps pipelines, without slowing down development efforts. It helps you automatically perform the right security tests at the right time, based on user-defined policies, risk profiles, and severity/context-specific code changes. And its risk-based vulnerability

"The net benefit we've found is less extraneous testing, which translates into less data to manage, less confusion trying to reconcile data from duplicate tests, [and] ultimately less stress on our resources. Intelligent Orchestration has allowed us to focus on higher-value tasks."

—Senior technical lead, Synopsys FSI client

See the full success story here.

“The format that Citi and Synopsys developed offers

Synopsys security testing services

Synopsys managed services help you accelerate and scale your application security testing strategy using on-demand resources and expertise.

If your organization develops software internally, you're doing so faster than ever before. It's likely that your team lacks sufficient application security skills and resources to sufficiently test your proprietary and third-party code. Synopsys security testing services provide on-demand access to security testing experts who have the skills, tools, and discipline needed to cost-effectively analyze any application, at any depth, at any time.

You can use managed services to strengthen your AppSec stance and fill in any existing gaps in your security initiatives. Managed services provide a shortcut to security, so you can protect yourself today.

Learn more about Synopsys managed testing services.

- Penetration testing. Find vulnerabilities in your applications and services before hackers do.
- Dynamic application security testing. Expert DAST, delivered on demand.
- Static application security testing. Respond to changing testing requirements and evolving threats with on-demand SAST expertise.
- Mobile application security testing. On-demand security testing, optimized for the unique risks of mobile applications.

To explore the complete Synopsys solution suite, visit our website to learn more.