RAPID7

CASE STUDY

Auden Group Relies on the Rapid7 Insight Platform to Securely Expand Its Financial Services Product Portfolio

InsightConnect, InsightIDR, InsightVM, InsightAppSec

Auden Group is a socially responsible financial services company. Through technology, research, and innovation, the company is building better ways for its customers to borrow and take control of their money. Founded in 2013, Auden's first product was a loan platform that makes short-term loans more affordable. Today, the Manchester, UK company is developing new banking services designed to improve customers' financial health and wellbeing.

The company's leadership recognized that cyber security was central to the success of its mission and growth. As a result, they brought on a six-person security team, led by Philip Wright, Head of InfoSec, to manage all aspects of cybersecurity from prevention to threat response.

The Greatest Threats: Phishing and Human Error

"I've been working in security for 12 years, dedicated to InfoSec," states Wright. "I'm concerned with every type of security incident. But I think the ones that scare me the most are phishing and human error." Wright wanted to build a program around the NIST cybersecurity framework: identify, protect, detect, respond, and recover. With only a month until the company's first product launch, Wright's priority was obtaining the ability to detect suspicious activity. He turned to InsightIDR - Rapid7's easy to deploy SIEM (Security Information and Event Management) solution that features built-in threat detection.

"You can't respond and recover unless you can detect," states Wright. So, within two weeks of starting at Auden, Wright began a POC of InsightIDR. He had never used InsightIDR before, but he had extensive experience with other SIEM solutions and he knew that it would take months to get to a point where one of those products would be fully deployed. He needed a product that had powerful out of the box detection capabilities. InsightIDR features User Behavior Analytics and a number of other detection methodologies, making it the perfect product for Wright's needs. "We were in production by day three of the POC and by the end of a 30-day POC, we were getting real value out of InsightIDR."

Doing More With Less

Challenged with building a SOC from scratch with limited headcount, once InsightIDR was up and running, Wright turned his attention to automating processes to keep his staff from being overwhelmed. "I looked at InsightConnect to address the automation challenge. And with it natively being supported in the same Insight platform, it really made sense for us to go that route instead of rolling our own or using a different automation platform."

Auden was able to quickly get more than 30 InsightConnect automation workflows into production. As a result, almost two-thirds of Auden's weekly alerts are handled automatically, while the remaining one-third are accelerated with automation and alert enrichment. "Before deploying InsightConnect we were getting about 300 alerts every week that we had to address manually," explains Wright. "With InsightConnect we have automated about 200 of them. We can automatically add context to the remaining 100 alerts, enabling our three SOC analysts to handle them more quickly and efficiently. It shortens our time to respond, and speed is of essence when there's a compromise or potential compromise."

One of the InsightConnect automation workflows uses Slack to validate whether a user performed certain actions. If the user says they did them, the investigation is closed. If the user says no, the team moves the investigation forward. Another workflow uses Slack to present pre-processed vulnerability analysis to the SOC team for analysis. The automation task runs a Slack-generated report of current critical vulnerabilities that can be handled by any of the SOC analysts. "It automatically kicks off a forensics workflow in Sophos, which we have on all our machines," explains Wright.

> ***"The only reason I can run a 24/7 SOC with three people is because of InsightIDR and InsightConnect***

"The workflow unpackages the specific machine's snapshot, sorts the data, puts it into a human-readable format, then makes the data query-able from Slack for the analysts. This saves about eight hours of work every time we run it – and we do this sort of analysis 3-4 times per week. That's a massive benefit."

The Benefits of a Comprehensive Platform

Once Wright had the tools in place to detect, respond, and recover, he needed to go back to the first part of the NIST cybersecurity framework and implement solutions to help identify and protect Auden's data and assets. For this, he turned to InsightVM, Rapid7's vulnerability management tool. One key benefit of the Insight platform is that the Rapid7 Insight Agent is used by both InsightVM and InsightIDR on Auden's endpoints. This meant that deploying InsightVM was fast and easy. It didn't hurt that the Insight Agent is very lightweight. "I hate agents unless they're lightweight and don't bog down the machine" says Wright, "and the Insight Agent is a true thin client."

Another benefit of using the Insight platform is the data that's exchanged between products. "Vulnerability and alerting data can be connected easily in an investigation. If we see any anomalous activity, we can immediately check for a relevant vulnerability in InsightVM," explains Wright. "We never have to leave our Rapid7 interface. We just click the drop-down into InsightVM and see if the approach is exploitable."

> ***"The bottom line is that when Auden's business is 10 times bigger, the security team won't need to be 10 times bigger. The Insight platform provides us with a lot of operating leverage and scalability***

Securing the Cloud

Auden's IT application deployment environment is completely cloud-based across (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It is critical that Auden's security program provides highly effective and consistent security controls across all three cloud platforms.

Auden is leveraging the native integrations offered by InsightIDR and InsightVM to help monitor their cloud footprint. They're also using InsightConnect to cut down on the legwork that would otherwise be required to manage security across their multi-cloud environment. For example, with assets spread across so many different types of infrastructure, it was a real challenge for the Auden team to understand if an IP address was internal or external, nevermind get details on the asset itself and where it was located. To solve this challenge, they built an InsightConnect workflow. Now the team can enter an IP address into Slack and the workflow will search through Auden's infrastructure to locate the IP address and associated asset. Once the asset is found, IP and asset details such as IP address type, asset name, asset type, location, availability zone, and more are provided in a Slack response. Auden also has a similar workflow to retrieve firewall rules.

The native cloud integrations found in InsightIDR and InsightVM, along with the dozens of cloud plugins offered by InsightConnect, make it possible for Auden to seamlessly manage security across their multi-cloud environment. "This is just one example of where the combination of monitoring, alerting, and automation combines to eliminate common mistakes before they can expose the company to a true security incident or require a report to their regulator," adds Wright.

As they continue development of innovative banking services, Auden is relying on Rapid7's Insight platform to provide a robust security environment. "The bottom line," concludes Wright, "is that when Auden's business is 10 times bigger, the security team won't need to be 10 times bigger. The Insight platform provides us with a lot of operating leverage and scalability."