RAPID7

Edinburgh Napier University

Chooses Rapid7 to Power Its CyberSecurity Team

Products

○ InsightIDR

○ InsightConnect

Industry

○ Education

Overview

The Company

Edinburgh Napier University is home to over 19,500 students from 140 countries. They study across three campuses in Edinburgh, and through online and transnational overseas education programs. The University was recently ranked the top modern university in Scotland.

Graeme Hamilton, Information Security Manager, is responsible for the University's information security infrastructure. That includes everything from administering security solutions and hardware appliances to user policies and awareness training, and security response activities. "The whole spectrum of information and security is my responsibility," notes Hamilton. "It's quite a busy role as you can imagine because we're only a team of three."

The Challenge

Hamilton and his small team are tasked with protecting the University's networks against the full range of security challenges, from unauthorized users to phishing attempts and cyber attacks. Not everyone on Hamilton's security team came from a cybersecurity background, so he looked for security tools which would provide his team with insights and support.

Another major challenge the team faces is the sheer number of students and the potential for missteps. "With almost 20,000 students, it was previously the case that our students didn't always have the best password hygiene. So, we would find that quite often their accounts would get compromised. We didn't really know what was happening because we didn't have robust monitoring to find that data. That is one of the factors that led us to look for security tools."

RAPID7

The Solution

A Powerful SIEM Out of the Box

Hamilton compared a number of SIEM vendors and deployment models and chose Rapid7 InsightIDR because of the powerful capabilities it delivers right out of the box. "We did not have to build out detections ourselves."

Implementing new security tools can be a daunting task for even the most experienced teams. But, for Hamilton and his staff, that has not been the case. "InsightIDR does an awful lot without us having to configure things. Deploying InsightIDR was incredibly easy in the sense that all we had to do was deploy the collectors on our network. We got the two collector servers deployed as virtual machines. We then configured a few of our systems as event sources to integrate with those collectors. And within a half a day it was all working."

Hamilton also points to the benefits of the Rapid7 software as a service model. "We didn't want to maintain the infrastructure ourselves - we didn't want to worry about servers or storage for SIEM data. Being able to just simply set up a subscription and start using it straight away, was really powerful. So, with almost no experience of our own, we have been able to reap benefits very quickly and easily with InsightIDR."

Hamilton notes that as part of his SIEM evaluation he asked a number of well-known vendors to provide time-to-value estimates. "They all said it would take significantly longer than what Rapid7 offered."

Insight Agents Provide Visibility and Control

The University has always had remote international users, but with Covid suddenly all 1,500 staff members were working from home. "That posed some interesting challenges for us," explains Hamilton. "We had to develop a whole new managed laptop service because traditionally our staff worked on desktop PCs in the office. We had a short timeline to get the laptops out to staff, and we had to roll out the service without compromising security."

That's where the Rapid7 Insight Agent proves invaluable. Regardless of what local networks those remote laptops are on, Hamilton and his team get the data from the endpoints. "And, as I said, the majority of these were on home networks but we were still getting the alerts and things from them as appropriate," states Hamilton.

RAPID7

> **"**
>
> **It's incredibly easy to get up and running with Rapid7. Within hour or days of starting to use InsightIDR, you'll begin to get quality actionable data. Rapid7 helps us manage our workload by giving us the ability to do more with less.**
>
> Graeme Hamilton, Information Security Manager

"Plus, we already had all the behavioral analytics features of InsightIDR, which meant that as folks were starting to work from multiple locations we got the alerts, telling us about that activity. And, we were able to tune those alerts and manage them to make sure that we were keeping on top of things but not being overwhelmed."

Hamilton adds that some peers are surprised at just how much detail his team can get. "But with the Insight Agent, you get the information. The Insight Agent has definitely helped us to detect things more quickly, and also come to a verdict more quickly as to whether or not something needs to be taken care of."

Hamilton and his team are getting alerts from things they would not have known about without InsightIDR – and they're able to resolve them satisfactorily. "We're not getting unnecessary alerts or getting overwhelmed by alerts that keep piling up. We're able to use the tools to investigate, make a decision, and deal with the alerts."

Automating Time Consuming Manual Processes

Hamilton next searched for an automation tool for their most time-consuming manual tasks. He found his solution in InsightConnect, Rapid7's security orchestration, automation and response (SOAR) solution.

"We identified use cases that didn't need to be done manually. For example, when we dealt with phishing emails, we were responding to users, investigating the messages, and taking action, which was very time consuming. We decided that anything we could do to automate and streamline that process would be helpful," he says. "That's where InsightConnect is really powerful because it brings multiple systems together and integrates them in a way that allows the automation to occur."

And another thing Hamilton likes, "We don't have to be full-on coders with extensive knowledge of programming." For Hamilton, it's all about making the process manageable for his small team. Having tools like InsightIDR and InsightConnect helps him do just that.

RAPID7

User Friendly Tools That Get the Job Done

"The Rapid7 products support my team and increase their ability to do more within their skill set and within the time they have available. They appreciate the fact that InsightIDR and InsightConnect don't require high levels of technical expertise. They are approachable. They are user friendly."

Hamilton also appreciates the fact that he has a voice as a customer into the process of improving the Rapid7 products. "It's great to work with a product that is being actively developed and improved. And to feel like we're valued customers who have a voice."

For anyone considering Rapid7's InsightIDR and InsightConnect, Hamilton offers this simple advice. "It's incredibly easy to get up and running with Rapid7. Within hours or days of starting to use InsightIDR, you'll begin to get quality actionable data. Rapid7 helps us manage our jobs by giving us the ability to do more with less."

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.
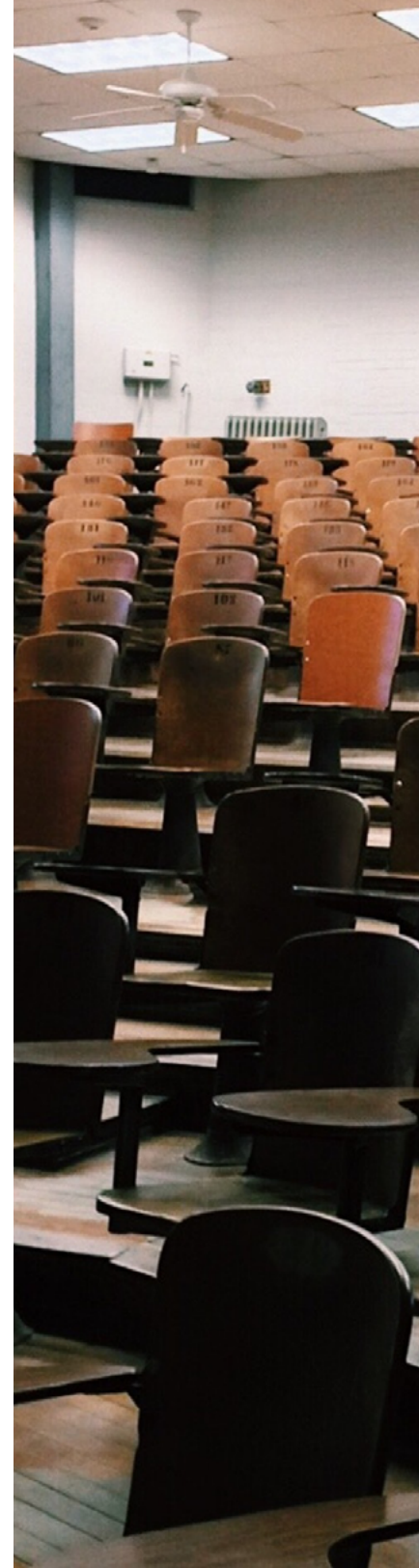
RAPID7

PRODUCTS

Cloud Security

XDR & SIEM

Threat Intelligence

Vulnerability Risk Management

Application Security

Orchestration & Automation

Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**