McGraw Hill Amplifies Security Efficiency With Splunk SOAR

Key Challenges

Without integrated security tools, McGraw Hill was manually responding to thousands of malicious emails every day, which slowed MTTR and increased the possibility of a successful attack or infiltration.

Key Results

By increasing automation with Splunk® SOAR, McGraw Hill has achieved faster response times, centralized investigations and event management, increased ROI and accelerated productivity.

Mc Graw Hill

Industry: Education

Solutions: Security & Fraud, Splunk Orchestration and Automation (SOAR)

Small teams need the right tool to work efficiently.

As a learning sciences company, McGraw Hill provides customized educational content, software and services for pre-school through postgraduate education. The organization also has a large digital products group that develops learning sciences platforms. McGraw Hill currently operates in 28 countries, has more than 5,000 employees globally, and offers products and services to over 135 countries in 60+ languages.

Because they provide an essential product globally, it is critical to McGraw Hill that they do so securely — and they learned how through experience.

"We had an incident where copies of our internal user addresses were released and received tons of phish exploiting this. There's no amount of people that are going to solve this problem. When something like this hits, the clock starts," says Jason Mihalow, Senior Cloud Cyber Security Architect. These incidents were monitored through a simple email inbox, and with few people to monitor this inbox, it was impossible to clear them all. "It's a completely manual process. When you experience a few of these waves where you're targeted, you come to realize that there's no amount of people that are going to solve that problem. Automation is the solution," says Mihalow.

Data Driven Outcomes

22 months
worth of manual security tasks automated within the first 6 months of 2020

10
Full Time Employee workload equivalent completed by small team within the first 6 months of 2020

9,439
security events resolved via automated response within the first 6 months of 2020

The right tool for the job

With Splunk SOAR, McGraw Hill is able to automate their response to threats like these. Now, the McGraw Hill team is able to put all of these reports automatically into Splunk SOAR, and pull them into a container. “A container case management based system prevents us from having to chase down emails in an inbox. We have everything in a single system and we know everything’s been addressed. We have a record of what happened, and what the analyst has done. This has been a generational leap for us,” says Mihalow.

Before Splunk SOAR, Mihalow says all of this information lived in 10 different tools, and in logs that are completely disparate. Consolidating this all into Splunk SOAR has been a huge help to the team. “Instead of having to go into other tools and do that blocking there, I’ve created playbooks that can automatically do that stuff. Analysts don’t have to leave Splunk SOAR to respond to the malicious emails,” says Mihalow.

This has saved McGraw Hill time training new analysts as they join their team. “Splunk SOAR has enabled us to consolidate our SOC. Before, when we hired someone, we said, ‘here’s your 10 tools and how to use them,’” says Mihalow. “Now, I can abstract all of that and just introduce Splunk SOAR. It brought all of our operations into a single place that we can maintain.”

> “There’s going to come a day that you’re going to be overwhelmed with the amount of work that you’re going to need to cover. There’s going to be a point where you can’t hire any more people. It’s humanly impossible to process the amount of data that needs to be processed, and the only path forward is automation.”
>
> **Jason Mihalow,** Senior Cloud Cyber Security Architect, McGraw Hill

> “Our gears have shifted since Splunk SOAR has been implemented. Any new process that comes in is always first viewed through the Splunk SOAR scope of ‘can we do this with Splunk SOAR’, and how much legwork is it going to take to do this without Splunk SOAR.”
>
> **Jason Mihalow,** Senior Cloud Cyber Security Architect, McGraw Hill

The Splunk SOAR advantage

Since McGraw Hill implemented Splunk SOAR, they have seen a lot of changes in how they handle security. “We have found many use cases for Splunk SOAR, not just those I’ve shared with you. In total, we have 40 something playbooks that I’ve created,” says Mihalow. “We use it for everything.”

These advantages don’t stop at use cases. McGraw Hill has seen an increase in ROI YoY, as well as an increase in the amount of work accomplished. When comparing the last two fiscal years, they have seen a $600,000 increase in ROI for 2020 to date, and expect that to reach nearly $1.6 million by the end of the year. “This is a testament to how much work Splunk SOAR is doing. We aren’t even at the number of events that we did last year, but you have so many processes underneath Splunk SOAR that in 7 months we are saving more than last year as a whole,” says Mihalow.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com