Chronicle SOAR

As the Crowe Soars

How a managed detection and response (MDR) provider got proactive about its security operations

Challenges

Crowe, a Top 10 U.S. accounting, consulting and technology firm, is consistently rated by Forbes and Fortune as one of the best places to work, largely because of its highly lauded culture, perks and values. The 30,000-employee firm also includes a digital security practice, which enables its many clients to become digitally safer places to work. That effort is especially bolstered by Crowe's managed detection and response (MDR) team, which helps customers monitor and quickly respond to security threats.

> "The analysts I talk to absolutely love Chronicle SOAR. This is because Chronicle SOAR automates the Level 1 work they would have performed that was monotonous and repetitive to them. This allows them to focus on higher-level tasks (and) deeper analytics and allows them to really get into the meat of security intelligence work."

Cameron Rayner, security intelligence center manager, Crowe

When the MDR service – which operates out of a security operations center (SOC) in Lexington, Ky. – was erected several years ago, Crowe wanted to ensure it was built the right way: powered by a security orchestration, automation and response (SOAR) product that would integrate all the disparate alert feeds the SOC ingests into a single pane of glass, allowing analysts to work cases more efficiently and empowering managers to more intelligently track their progress.

"As we began building the current generation of our Crowe MDR platform, we really wanted to make sure we were ahead of the game," said Glen Combs, security consulting partner at Crowe. "We decided that we wanted to start with a SOAR product."

Time to Respond

Volume of manual processes and inability to group similar alerts

Evaluation

Difficulty in measuring analyst productivity from a single dashboard

Visibility

Tracking all cases and investigations and adequately communicating with clients

Chronicle SOAR

Solutions

After considering several options, Crowe was drawn to Chronicle SOAR because of multiple distinct differentiators. In particular, the workbench's "threat-centric" approach to alert handling was the deciding factor.

Traditional SOARs are "alert centric," meaning alerts are treated in a vacuum. An alert comes in, a playbook runs, and an alert comes out – with no awareness that other alerts even exist. This leads to inevitable problems, notably unsustainable manual and redundant work by analysts.

In Chronicle SOAR, the starting point and the outcome delivered are drastically different. Before initiating any playbook, Chronicle first, and continuously, analyzes each alert as it comes into the product, looking for contextual relationships. If a relationship is identified, the alert gets automatically grouped with the related alerts into a case. "Before having that in place, it was a lot of manual work," admitted Kiel Murray, security engineering manager at Crowe.

Wins

Chronicle SOAR has enabled Crowe to automate common actions that once took five to 10 minutes to seconds or less. These can range from blocking a threat on the firewall to isolating hosts that generated malicious activity to performing WHOIS lookups.

As proof, Crowe measured logs entering its SOC, alerts triggered and escalated, and investigations launched – and noticed a remarkable 80 percent reduction in analyst caseload from before it lauched Chronicle SOAR.

And of those cases that must be managed, the Crowe MDR team can do it smartly thanks to the product's capabilities that enable automated alert grouping and case creation, continuous case prioritization and case assignment recommendations. This allows Crowe to effectively communicate concerns with clients, which is "the most important thing we can do," Combs said.

The goals that Crowe came in with prior to deploying SOAR from Chronicle and the success that has now resulted has left it considering the partnership as essential. "If Chronicle SOAR went away, our ability to do what we do today would cease," Combs said.

Respond in minutes instead of hours

80% reduction in analyst caseload

Improved decision-making by analysts and managers

Analysts freed up to work on other areas of threat detection