SIEMonster SIEM for Everyone

Case Study BlueScope

BlueScope is a global leader in the steel industry and is the third largest steel manufacturer globally. With over 14,000 employees in over 100 facilities around the world, BlueScope continues to grow and currently has offices in 18 countries. This translates into over 20,000 endpoints with an initial 100,000 EPS rate (currently 350,000 EPS) that needed security events captured. Such a complex and large-scale cyber security challenge requires an all-inclusive and flexible Security Information and Event Management (SIEM) solution. Unsatisfied with the price and scalability of the options available on the market at the time, BlueScope's Group Manager for Information Services and Cyber Security, Mr David Johnston, approached Chris Rock, Co-founder and CISO of SIEMonster, to find an alternative.

The Challenge

Mr Johnston of BlueScope had long wanted to build a Centralized Security Operations Centre (SOC) but was disappointed by the commercial security-intelligence options, describing them as "expensive and over-prescriptive". Mr Johnston shared his thoughts with the small team of professional hackers that were charged with BlueScope's regular pen testing exercises. Amongst that team of hackers were the co-founders of SIEMonster, and the novel concept of an affordable and infinitely scalable SIEM solution was born. The team of the newly founded SIEMonster then worked closely with the security team of BlueScope for two years to build them an affordable, scalable SIEM solution that could monitor servers, routers and firewalls, as well as complex SCADA systems, like blast furnaces and automated heavy equipment.

Mr Johnston explains that BlueScope needed continuous monitoring and alerting capabilities but couldn't justify the cost of the solutions at the time. He admitted that BlueScope had had a "pretty tough few years and were quite challenged in terms of cost... Looking at the marketplace, software costs are in the hundreds of thousands". He also expressed frustration at the installation time and costs: "By the time you get a project team in to do the integration, it's usually $1 million plus."

In an attempt to curb unnecessary costs, SIEMonster CISO Chris Rock turned to open-source options including the Elastic stack, Kakfka, Wazuh and other open-source projects.

These combined tools provided the security team with real-time visibility of BlueScope's entire network and allowed administrators to set thresholds and alerts/flags for specific actions. The trial was successful, and the solution continued to evolve.

"It was beyond our expectations in terms of just how well and how smoothly the trial went," Johnston says.

The Solution

The solution put forward by the team that now forms SIEMonster was first implemented in April of 2015, and continues to this day. BlueScope currently uses SIEMonster's Enterprise Edition and is grateful for the continued incident visibility and protection it affords.

"Given the way the world is going and the way the threat landscape looks these days, it really is important to have that real-time view of what's going on."

BlueScope's SOC has been processing over 350,000 Events Per Second (EPS) using SIEMonster's solution, from across their worldwide network. Mr Rock explains that "data is filtered and made available to the users in real time, with around 10TB of processed data expected to be produced and archived every month".

SIEMonster's production environment is built on Kubernetes and leverages Amazon Web Services' Elastic Cloud 2 (EC2) and Simple Storage Service (S3) to scale its virtual-server and data-storage infrastructures with demand. The solution was initially designed to store around 12 months' data onsite, with an additional 12 months' data archived and a further 12 months' data potentially being offloaded to Amazon's Glacier at-rest storage service for later recall as needed.

SIEMonster's solution also provides a historical data set that can be viewed alongside with current activities to foster invaluable correlation for reporting on organizational performance.

Due to the open-source design of the solution, the team were able to integrate a diverse range of systems with ease. This was imperative due to BlueScope's heavily industrialized production environment. With SIEMonster's unique design, the SOC were able to monitor much more than just standard systems such as payroll systems or networked devices; They were able to oversee industry specific control systems that BlueScope uses, such as systems attached to steel furnaces and paint guns.

Siemonster's affordability, scalability, and easy visualisation made for the perfect solution to BlueScope's unique security problem.

About SIEMonster

SIEMonster was established in 2015 by a team of professional hackers with more than 20 years of experience in the industry. We are the only SIEM company in the world that offers affordable SIEM solutions, no matter the size of the company. Significantly faster than our competitors at logging and analyzing Events Per Second, our product is very efficient, which can save our customers millions. SIEMonster's dashboard provides easy visualization and real-time alerts to modern day devices and applications, such as Slack and SMS, as well as white labelling to its clients to ensure a comprehensive brand experience.

Find out how SIEMonster can help you at siemonster.com