Stage 2 Security

By taking advantage of SOC Prime's Detection as Code platform, Stage 2 Security has reduced by 50% its MTTD using up to hundred queries per second in the company's daily SOC operations.

Industry	Region	Company Size	SIEM & XDR in Use
Security & Investigations	**USA**	**11-50 employees**	**Elastic Stack**

Jake Groth
Chief Technology Officer

"The biggest thing SOC Prime does is reduce the number of hours we need to spend on detection content development, which enables us to focus more on security operations. With the SOC Prime Threat Detection Marketplace, we've managed to achieve really low mean time to detect (MTTD) and reduced the burden on our SecOps Team."

Highlights

- Stage 2 Security (S2) selected SOC Prime as a scalable solution to augment daily threat hunting operations
- Partnership with SOC Prime helped the company's SecOps Team reduce their MTTD by 50%
- Leveraging an API Integration tool, S2 enabled automated threat hunting by obtaining thousands of use cases that scale with the customers' needs
- S2 managed to continuously obtain high-quality SOC content tailored to the company's custom use cases

Challenges

Tailored Behavior-Based SOC Content. Having sufficient experience in delivering SOC operations in the private and public cybersecurity sector in the USA, Jake Groth, the CTO at S2, has noticed that now clients are more focused on the actual detection content tailored to the company's infrastructure and threat profile. While there is a great number of trained SOC Analysts who know how to respond timely to the incoming alerts, there is always a problem finding relevant content applicable to the company's SIEM solution with proper behavior indicators.

Talent Shortage and Content Scalability Issues. Threat Hunters are really hard to chase on the market, and even if companies have managed to find them, it is still challenging for individual content contributors to keep pace with the crowdsourcing SOC content library with hundreds of authors, such as the Threat Detection Marketplace. Apart from this massive talent shortage in the security industry of SIEM Content Developers and experienced Threat Hunters, their produced content doesn't always scale with the company's business.

High Cost of Content Outsourcing. S2 found that ordering external content development services wouldn't be reasonable enough for the growing company. In addition, transitioning outsourced detections to various SIEM, EDR, and NTDR language formats brings about another financial challenge.

Automation and Industrialization. Automation and industrialization are familiar concepts across the entire IT sector. In cybersecurity, processing hundreds of queries per second requires automating and industrializing threat hunting for more efficiency. Stage 2 Security was looking for automated solutions that would scale out a lot of parallel processes and augment its threat hunting operations. Possessing high-skilled staff with sufficient expertise in content development was not enough for S2 to compete with the speed of Detection-as-Service platforms. Therefore, Stage 2 Security was looking for similar product vendors that enable Continuous Security Intelligence to help organizations augment their development potential.

Solution

While searching for a way to address all the above mentioned challenges, S2 found that purchasing the SOC Prime Threat Detection Marketplace license would unlock the opportunity to obtain the high-value curated detection content on a regular basis. S2 found it more reasonable to obtain scalable Detection as Code content from SOC Prime rather than fully manage security content development in-house, essentially saving on having dedicated CTI and research specialists and focusing more on Incident Response, Threat Hunting, and Content customization to meet the customer needs.

Achievements

API Integration

S2 has mainly taken advantage of the API Integration tool for automating the detection search and threat hunting operations. The company has simplified its content development to a minimum number of steps:

- Pulling down content via API
- Enriching detections
- Deploying detections to relentlessly hunt customers' data at scale using DevOps pipelines

High-Quality Customer Engagement

SOC Prime Team is striving to be highly responsive to the company's feedback. S2 has mentioned that "customer engagement is great", proving that SOC Prime is really trying to make its product better.

Content Update Notifications

The regular SOC Prime's practice of sending email notifications of the latest detection content releases helps staying constantly updated and allows quickly getting "the hottest" detections to make sure the company's customers are protected.

Emergency Attack Coverage

S2 hugely benefits from the content coverage of the emergency attacks like the SolarWinds use case. As a slight improvement, S2 sees adding alerts that would notify the SOC Prime Threat Detection Marketplace users that they are a couple of hours away from having their SIEMs updated on the most recent detections.

Threat Hunting Made Easier

SOC Prime genuinely helps make threat hunting easier and more accessible, which allows gaining more control over implementation and customization of detections and completing these operations in-house.

Cloud Security Use Cases

Content categorization based on security use cases seems like an asset for Stage 2 Security since the company is mainly providing cloud security monitoring for its customers. Increasing an amount of cloud-native detections can notably enrich most SaaS, IaaS, and PaaS solutions.

About Stage 2 Security

Stage 2 Security (S2) was founded by the former National Security Agency (NSA) security experts in 2014 and since then the company has been delivering managed protection services, including SOC-as-a-Service and Vulnerability Management, Adversary Simulation involving Red

Teaming and Penetration Testing, Adversary Prevention, Cloud Security Monitoring, and Incident Response operations. S2 describes its mission as "Instilling security through expertise and innovation" striving to combine the seasoned expertise of its founders with a drive for applying state-of-the-art technologies to enhance the company's daily SOC practices.