Pokemon Go

MOBILITY > MOBILE MANAGEMENT AND SECURITY

Pokémon Go Sharpens Its Security Game by Building a Security Operations Center

Building a security operations center was just one of the steps taken to turn Pokémon Go into a tech company.

Karen D. Schwartz | Mar 03, 2019

When John Visneski joined Pokémon Go as director of information security and data protection officer in mid-2017, he didn't expect too many similarities with his years as an information security specialist for the Air Force. He was wrong about

At the time Visneski came on board, the company was experiencing explosive growth that continues today. As of last year, the mobile augmented reality game has been downloaded more than 800 million times and has 5 million daily active users. Growth at Pokémon Go came so fast and so furiously that it strained the staff of about 10 IT specialists to the breaking point. To accommodate that growth, Visneski essentially chose to turn the organization into a technology company overnight, filling out the IT staff with dozens more DevOps engineers, application developers and security specialists. He also decided to build the company its first security operations center (SOC).

The main goal of a SOC is to protect the information systems of an organization. Typically, a company achieves this by consolidating data, systems, tools and security experts in a central location. Yet some SOCs aren't as effective as others. David Monahan, research director of security and risk management at Enterprise Management Associates, said that an effective SOC must be fully automated, have solid processes and procedures, employ well-chosen and architected tools, and empower personnel to make and execute decisions appropriate for their positions.

People, Processes and Technology

For Visneski, building a SOC from the ground up was a chance to choose the best processes and tools. He chose to build a foundation by fostering long-term relationships with a few core vendors—in this case, Sumo Logic and Crowdstrike. These tools provide the bulk of the capabilities, including identifying and prioritizing threats, neutralizing security vulnerabilities, log aggregation and security analytics. For the rest of the architecture, he took a shorter-term approach, which allows the SOC to quickly change course with new tools as threats change. These include tools for file integrity monitoring, data loss prevention, code scanning, secret key management and endpoint protection. Together, all of these tools provide correlated visibility, attack surface management, identity management and incident response.

security in so you don't have to bolt it on later, which opens things up to vulnerabilities and is cost-prohibitive."

Building up the SOC team with experienced security professionals was a smart move. Highly trained and certified staff with relevant experience, especially those who can adapt to changes quickly and learn on the fly, is critical to an effective SOC.

And make sure you keep your staff's knowledge—and your tools—current, Monahan said.

"The processes, procedures and technologies you deploy will change over time, so it's not a set-it-and-forget-it thing. It's constantly evolving. And you'll figure out a better way to solve a problem," he said. "It's a living, breathing entity that changes over time—and it should."

What Not to Do

While this advice will make a good security operations center better, there are plenty of things that can drastically reduce the effectiveness of a SOC. One of the most common is poor monitoring architecture, which causes tool or data silos. Another is relying on processes that have gaps or other flaws that allow important vulnerabilities to fall through the cracks. Worse yet is automating these bad processes.

"Automation allows the team to execute faster, but automation on top of a poor set of processes only allows delivery of poor outcomes more quickly," Monahan said.

A recent SOC report from the SANS Institute pointed out even more mistakes organizations make. One is lack of automation or orchestration. In other words, if your tools aren't well integrated, they can't do their job effectively.

those tool sets are orchestrated in such a way that your team can actually leverage them to a high capability, you'll be in trouble."

The SANS Institute report also found that most companies should reconsider their existing their asset discovery and inventory tools, a tool set that was rated the lowest of all SOC technologies in use. The report also found that most event correlation continues to be manual, and should be automated when possible. Finally, the report found that most SOCs suffered from a lack of skilled staff.

But, when done right, you might even gain benefits you didn't expect. At Pokémon Go, Visneski quickly realized that the log aggregation and data analytics capabilities the SOC was using for its security operations also could benefit the company's business, intelligence and application studio areas.

"We realized that being able to take in data feeds from all of these different areas and put them in the same place using dashboards gave us visibility we didn't have before, and that's really powerful--not just for the security team, but for the business at large," he explained. "In fact, our second-biggest user today of Sumo Logic is our game studio designers. They find that they have more visibility into their own data. That, in turn, makes us more secure because it gives security more visibility into the data overall also."

There is a world of potential in a well-designed SOC and a great team of people, Monahan believes.

"It comes down to what do you want to get out of your SOC. Do you want it to be simply a ticket jockey, or do you want it to provide other value-added services to your business? Most SOCs tend to focus on fighting fires, but it can be more than that. Get out of firefighting mode and into a repeatable operations process, and make it a useful organization as opposed to just a firefighting organization," he said.

Go's SOC with Sumo Logic's.

"It's about what best practices, processes, alerts and tactics we can share to make us both better," he said. "If they see something we haven't seen yet, we want to be able to get that information quickly so we can improve our own security posture, and vice versa."

TAGS: SECURITY

0 COMMENTS

RELATED

He Said What? Deep Learning Changes the Game for Social Engineering Attacks
FEB 27, 2019

New Approach to IDaaS Fights Hackers on Multiple Levels
FEB 16, 2019

RSA 2019: Is Your Company Getting Security Awareness Right? Probably Not.
FEB 13, 2019

City of Las Vegas Makes Bet on Advanced Threat Protection Solution
FEB 13, 2019

Follow us: