splunk>

CASE STUDY

Automating Phishing Investigations at the No. 1 Managed Cloud Company

Executive summary

As the world's leading managed cloud company, Rackspace has more than 6,000 employees and an infrastructure that spans four continents. Investigating phishing emails is just one of many issues the security team addresses. Rackspace needed a security orchestration, automation and response platform, and selected Splunk Phantom. Using Phantom's Apps and Playbooks, Rackspace is now able to quickly execute actions, ensuring a repeatable and auditable process for investigating and remediating phish. Since deploying Phantom, Rackspace has seen benefits including:

- Automating a manual process that required up to 10 different security products and took 90 minutes or more
- Increasing efficiency, consistency and improving security
- Freeing the team to focus time on investigations that require human insight

Why Splunk Phantom

At Rackspace, a typical day might bring as many as 45 phish for the security team to investigate, and the standard operating procedure for this type of event includes acknowledging receipt from the employee, assessing important details such as the sender, and taking steps to remediate if the phish is confirmed to be malicious. From start to finish, the process might take more than 90 minutes for each phish.

While even a typical day brings a nearly unmanageable workload, the team occasionally sees burst attacks with up to 300 phish in a single day. At this rate, it's easy for analysts to become overwhelmed, causing speed and consistency to suffer in the heat of the moment.

In addition, when it's necessary to collaborate with teams outside of security, the process slows down even more. For example, working with the IT group after normal business hours to pull a questionable email from the Exchange Server could triple the time required to handle a phish.

Rackspace began searching for a platform that could help automate and orchestrate the handling of phish and other security issues. Though flexibility was important, the company needed a product that didn't require DevOps resources to be successful. After considering its options, Rackspace adopted Phantom.

Industry

- Technology

Splunk Use Cases

- Security Orchestration, Automation and Response

Challenges

- Needed a security orchestration, automation and response platform to improve security

Business Impact

- Saving time by automating and orchestrating the management of phishing incidents and other security issues
- Simplifying workflow across security and other teams
- Gaining flexibility to address the company's dynamic network without requiring specialized DevOps skills

Splunk Products

- Splunk Enterprise
- Splunk Phantom Enterprise Edition

Security automation and orchestration with Phantom

A Phantom Playbook is triggered when a suspected phish is received. As the sender may target multiple employees, Phantom's first order of business is to search Jira for similar cases under investigation and query Splunk Enterprise for similar emails in the logs. Next, Phantom orchestrates a URL lookup and checks the file reputation on VirusTotal, and then pulls a domain and IP reputation from PassiveTotal. If the email includes an attachment, Phantom detonates the file in FireEye and Wildfire sandboxes before updating the Jira ticket with all information collected in the investigation. As the investigation playbook completes and analysts take over, the team has the information it needs to review the event and determine action quickly.

Rackspace adopted a modular approach to playbook development, which aids in making its Phantom implementation agile. For example, a second playbook that executes pre-approved quarantine actions can be triggered after the phishing investigation playbook completes. The same quarantine playbook can also be used with other security events beyond phishing. The same modular approach allowed Rackspace to start quickly with a simple playbook while working with Phantom's delivery services team to mature the overall deployment. As new Phantom Apps are introduced into the community, the number of playbooks Rackspace uses will continue to grow.

Fast and accurate phish resolution

With Phantom, Rackspace has been able to reduce the time required to handle phish dramatically. What once was a manual process that could take 90 minutes or more per phish, now completes in under a minute, freeing the team to focus time on less routine investigations that require human insight.

"Splunk Phantom helped us automate a process that used up to 10 different security products and took an analyst 90 minutes or more to complete manually."

David Neuman, VP & CISO
Rackspace

Burst attacks with hundreds of phish in a single day are now managed with consistency and little disruption to the team. With a Phantom Playbook, the same data is gathered for every phish, and every phish is investigated the same way, every time.

Codifying the process to engage with teams outside of security through pre-approved playbook actions results in a workflow that is greatly simplified. Competing priorities, after-hours requests, and other issues that might cause delays in a coordinated response are a memory now.

As the first community-powered security orchestration, automation and response platform, Phantom gives Rackspace the flexibility to address its dynamic network without requiring specialized DevOps skills. For example, the Automation Editor assists users with the creation of playbooks independent of an analyst's knowledge of programming, and Phantom Apps are available for a wide range of point security products that are available today. The Phantom platform then ensures that both the apps and the playbooks integrate seamlessly with one another.

Beyond the tangible benefits of efficiency, consistency, and improved security, Rackspace chose Phantom based on the company's willingness to collaborate and commitment to mutual success. It's a partnership that started strong and continues to flourish each day.