CASE STUDY

Tanium accelerates GoDaddy's security and incident response team and reduces IT outages

Jason White, Director of the Computer Security Incident Response Team (CSIRT) at GoDaddy, had a problem. His eight-person team was adept at identifying threats and compromises of their systems, but they were unable to scope incidents quickly with their existing endpoint security tools and couldn't trust they had a complete picture from all of their endpoints. As a mobile-first workforce where employees are provided laptops instead of desktops, GoDaddy had increased their risk of unwanted software entering their environment from home, affectionately called "Bring Your Own Malware." "What keeps me up at night is the thought of not finding an intrusion before it becomes data exfiltration," said White.

After hearing about Tanium at a security practitioner conference, the team requested a demo and was impressed with the platform architecture and speed for scoping and remediating incidents. They began the procurement process soon after because he realized he could "know within seconds and minutes versus hours and days" what was happening on his network.

Tanium use cases

- Security Hygiene
- Endpoint Security
- IT Operations Management
- IT Asset Visibility

Challenges

- Timely response to security incidents
- Lack of visibility across endpoint security tools
- Malware removal
- Ability to address vulnerabilities quickly
- Visibility to isolate and remediate a network outage

Benefits to IT

- Reduced time to remediate IT outages
- Faster reaction time to detect and remediate malware instances
- Decreased the mean time to recover
- Ability to investigate an endpoint remotely in real time
- Overall increased IT administrative productivity

Quick visibility enables proactive hunting and security hygiene

GoDaddy has since deployed the Tanium Core Platform and many of the Tanium Security Suite modules. Deploying Tanium has helped GoDaddy to automate ad hoc and indicator of compromise (IOC) searches, quickly implement blocked hashes, deploy patches at speed and scale, and create queries on an hourly basis to look for changes as a means for investigation. "We can now automate what we know to spend more time looking for what we don't know, and ultimately then automate that," said White.

Security hygiene is another key issue where Tanium is used extensively. In particular, Tanium is used to continuously monitor for out-of-date versions of typically exploited applications like Java and Adobe Flash. Once identified, remediation can be done immediately using Tanium. Before Tanium, vulnerabilities couldexist for days before being addressed in normal patch cycles.

Exponential reduction of mean time to recover

Because GoDaddy is a highly customer service driven business, mean time to recover is an incredibly important measure for the company. Mean time to recover is measured from initial issue to getting customers or employees fully back online.

Since deploying Tanium "hunting has also changed dramatically," said White. Historically, GoDaddy used their security information and event management (SIEM) system as the primary tool to hunt. "Previously, once we saw an indicator, we would do more reports to investigate, pivot, and do this over and over. It was an iterative process that took way too much time." With Tanium, GoDaddy is able to take each SIEM alert and immediately obtain more context through the ability to query affected endpoints such as running processes, registry settings, or open network connections. "Now, we can investigate a machine remotely in real-time with Tanium."

Beyond detection and initial investigation, quickly scoping an attack was another key need for GoDaddy. The team realized that attackers usually go beyond an initial compromise to move laterally. Working with reports and pivoting to get new data sometimes took as long as 24 hours. Scoping also took numerous iterations, which made it critical to gather data very quickly.

The CSIRT team can now detect and respond to incidents programmatically and have dramatically decreased the mean time to recover from an incident. "With Tanium, we can put together an action set that has each server test itself, then package with a script that's run locally with Tanium that can output a report on status," said White.

Beyond security

After implementing Tanium primarily for security, the team found that Tanium was also very effective in addressing a number of IT operations use cases, from end user support to IT asset management and M&A consolidation.

Recently, GoDaddy had a spanning tree loop that caused an internal network outage. This error was related to a known issue with Mac Thunderbolt monitors—but the operational support team didn't know which endpoints were using this monitor, and the issue seemed to come and go. Using Tanium, a team member asked "What machines are running Thunderbolt monitors?" and got the answer back immediately. Leveraging Tanium, the team correlated the event of a specific monitor being plugged in with the network outage, which was the key data point needed to isolate buggy displays.

Ultimately, White envisions tapping the power of Tanium to automate systems support. By identifying memory and disk space issues on servers in near real-time, White's team can react quickly to issues that could negatively impact a customer's business before they happen. Tanium has the ability to triage the issue before any servers go down. Jason explains: "Our vision is to leverage the API side to automate questions, and then turn it around to perform actions in the environment. This will allow us to fully instrument repetitive tasks, giving the team moretime to hunt for things that we don't know about."