Censys

Customer Case Study

How a Security Team Automated Attack Surface Management

Censys

How a Security Team Automated Attack Surface Management in the Age of Remote Work

From your hybrid cloud environment to your remote workforce, protect your attack surface with the Censys Attack Surface Management Platform.

See a Demo

Censys Products

- (ASM) Censys Attack Surface Management Platform

Introduction

Censys partnered with a State agency soon after the Covid-19 pandemic hit. New challenges emerged with the vast workforce moving to a remote working state. Cisco estimated a 25% increase in cyber threats or alerts since the pandemic began.[1] The state agency has a 78 person staff and a small security team. They have an important mandate: to provide technology, fiscal analysis, and legal support to the Indiana General Assembly. The security team had heard of Censys through OSINT training and were looking to scale their risk management program by automating attack surface discovery and tracking. They needed a tool that could give them the highest confidence and peace of mind that they are effectively protecting all the things that belonged to them on the Internet.

Attack Surface Changes with an Increasing Remote Workforce

Our customer is a leading innovator at the state level, and like many organizations, had a number of compounding factors impacting their attack surface simultaneously. The first of which was the influx of remote staff working from home, outside of the traditional network boundaries setup and secured by the organization. In the word's of the Chief Technology and Security Officer, "We are looking at expansion of our endpoints with several people working outside our firewall. Before, we had a small part of our staff that had laptops that took laptops home and that's just increasing now." This is not a unique story these days when it comes to managing a remote workforce. Visibility of your "end points", even outside of the traditional perimeter of the organization, is critical to an effective security program.

[1] Cisco, Future of Secure Remote Work Report.
https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-remote-worker-solution/future-of-secure-remote-work-report.pdf

Protecting your Attack Surface through a Complex Cloud Migration

Like many organizations, they were also concerned about securing their infrastructure. The security team was in the midst of migrating some assets from a traditional datacenter hosted by the government to a new provider on their private cloud. On top of that, they were preparing to move additional resources to Amazon AWS infrastructure. During any migration, it is critical to ensure the secure transfer of all your data. In particular, ensuring your servers and anything touching the public Internet are properly configured and accounted for as you create and wind down components of your infrastructure.

Leveraging Censys to Continually Monitor Assets from an Adversary's Perspective

Attack Surface Management (ASM) is the continuous process of discovery, inventory, and resolution of risk impacting your Internet-facing assets. Organizations are constantly reshaping their Internet-facing attack surface, whether they know it or not. Services, and the data those services utilize, are being developed, deployed and re-configured across the Internet, many times a week. Whether on your public cloud instances, on-prem servers, or on Third Party managed infrastructure, the task at hand has become much more complex and difficult in recent years.

In the words of the the CISO, Jeff Ford: “We knew that our threat surface was increasing and we wanted to make sure we were using tools, specifically Censys [ASM], to understand what that threat surface looked like.” What does that mean for the day-to-day of the security practitioner? The state agency operationalized the findings from the Censys ASM Platform in the following ways.

- **Ongoing Port Scanning to Mitigate Threats to External Servers -** The team at the state agency is now using the Censys ASM Platform to look for exposed ports/protocols on public facing servers. As their InfoSec Analyst stated, “We were saying, right, do we need all these ports up and running, or is it something we should change?” This allowed the team to quickly and effectively reduce their attack surface, labeling specific hosts as allowed to have certain ports/protocols open and continuously monitoring for security posture drift moving forward.

- **Tracking an Expanding Attack Surface with Employees Working from Home -** With increasing numbers of employees working from home outside the company firewall, there can be new cybersecurity threats and blindspots when it comes to network security. The state agency wanted greater visibility into the endpoints of their employees logging in everyday -- where were they logging in from and how this was impacting their attack surface. Expanded visibility through the Censys ASM Platform allowed them to protect employees working from home by monitoring for potentially exposed services that shouldn’t be.

- **Certificate Management to Ensure Business Continuity -** In the words of the state agency's security analyst, "The certificates expiring is a nice reminder that we see what we have expired and what we don't." Censys collects unique certificates and analyzes them to indicate how widely they are trusted, their level of encryption, if they are self-signed, and their expiration. This process can highlight potential security problems. Censys collects certificates through internet wide scanning and synchronizing with Certificate Transparency logs for comprehensive coverage. The State of Indiana's vigilance is important because an expired certificate could inhibit the ability to run secure transactions online.

- **Improved Cloud Visibility to Combat Configuration Mishaps -** As the state agency migrates and expands their cloud environment in the future, there are always concerns about misconfigurations and unsanctioned cloud services being provisioned and used by staff. Through the Censys ASM Platform's cloud connectors, the organization will gain additional visibility and security insights into their new cloud environment by identifying things like: exposed S3 buckets (or other object storage), unsanctioned cloud accounts outside of the security team's control, as well as exposed services in cloud environments like databases and RDP. Cloud connectors allow them to easily track these assets over time, measuring the security changes enacted and deployed.

Censys Provides Time Savings and Peace of Mind for Security Practitioners through Automation

Prior to using Censys, the state agency did not have the human power and resources to manually track their attack surface effectively. With severe resources constraints, automation becomes even more important in the realm of information security and risk management. There are not enough hours in the day to do the caliber of monitoring and risk management required for a quickly changing attack surface. In the CSO's own words, the only option was to adopt tools: "We really focus on giving [our team] tools that allow [them] to do all the work." Now their organization can keep track of its assets, unsanctioned IT environments in the cloud and beyond, as well as potential risks affiliated with certificate and domain expiration, potential vulnerabilities, and other misconfigurations.

Conclusions

Securing an organization of any size takes the convergence of people, practices, and the right tooling. The state agency has a suite of security tools to help as part of building their cyber resiliency, but the Censys ASM Platform remains a critical piece to this puzzle. As they complete their migration to the cloud, the Censys ASM Platform will play an increasingly critical role, illuminating attack surface vulnerabilities and empowering their security team to manage their constantly changing environment.

For more information about our Censys ASM Platform **visit our site**.