PRESIDIO®

CASE STUDY

StartingPoint
Managed Cloud Services

THE CUSTOMER

StartingPoint is a SaaS customer operations and experience platform for service-based companies, firms, and teams to simplify customer on-boarding, project management, helpdesk and service management, team management, and communication. StartingPoint is designed to help companies provide an amazing customer experience after they gain a customer by providing companies and teams an efficient, lean customer operations platform that can be deployed, customized, and leveraged quickly. These core values help companies and teams decrease customer churn, retain their customers, ensure high customer satisfaction, and increase team productivity.

THE CHALLENGE

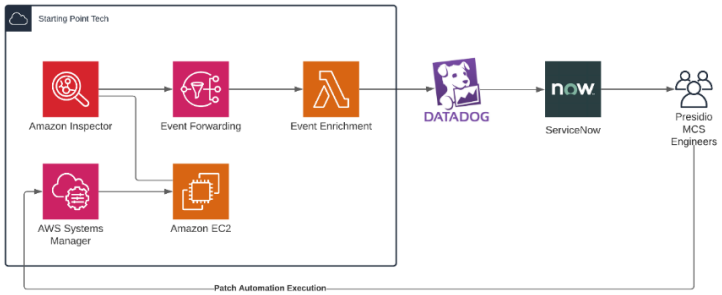
As a provider of hosted software, maintaining customer trust is very important. Using components with known vulnerabilities is one of the top 10 web application security risks highlighted by the industry recognized OWASP Top 10 list for 2019. Setting configuration and compliance standards and continuously inventorying software components against sources like CVE helps identify vulnerable software components and rapidly update them. Maintaining customer trust in the service that StartingPoint delivers is a key driver for StartingPoint's focus on this area of security.

StartingPoint worked with Presidio to ensure their EC2 instances do not have any high severity findings, remediate those finding through patching & configuration changes, and schedule weekly scanning using the Amazon Inspector CVE Rules Package to ensure their EC2 instances stay hardened and any new CVEs are addressed quickly.

HOW PRESIDIO HELPED STARTINGPOINT SOLVE THE PROBLEM

Presidio deployed Amazon Inspector, creating an assessment template scheduled to run the CVE rules package on a weekly basis. Notification of high severity findings from the weekly Amazon Inspector assessment was configured to raise an event in Datadog and a ServiceNow ticket for Presidio Managed Cloud Services.

After the initial execution of the assessment on October 9, 2020, Inspector identified several high severity findings across the StartingPoint EC2 landscape and incident ticket INC7548838 was opened in ServiceNow. The ticket contained a list of the high severity vulnerabilities including, among others, CVE-2019-7306 for the Linux application Byobu. Presidio scheduled an initial patch execution through AWS Systems Manager Patch Manager remediated these vulnerabilities. This resolved the initial Inspector findings.



AWS Systems Manager Patch Manager was scheduled to run in a monthly maintenance window to install security updates periodically. Further, Presidio Managed Cloud Service' robust SLAs for incident response and remediation drive quick action by its engineers to assess and remediate incidents for high severity Amazon Inspector findings rapidly and thoroughly.

PRESIDIO®

CASE STUDY

StartingPoint Managed Cloud Services

SOLUTION OUTCOMES

Prior to implementing these Amazon Inspector and AWS Systems Manager Patch Manager, StartingPoint had unknown high severity vulnerabilities within its infrastructure. Now, patching is performed on a regular basis with consistent results and predictable, automated detection when out-of-cycle patching may be needed to address a high severity finding.

StartingPoint has a significantly improved security posture through their partnership with Presidio Managed Cloud Services. Through this work, StartingPoint adds another capability needed to move forward with compliance standards or regulatory certification they wish to pursue in the future.

In summary, by working with Presidio Managed Cloud Services, StartingPoint has:

- Significantly improved their security posture in the cloud
- Decreased detection of insecure configurations from weeks to seconds
- Decreased time-to-remediation of resources not complying with policy from days to hours
- Built a strong foundation for future compliance or regulatory certifications like SOC2, PCI, etc.

Visit us online today or call us at 800.235.6259