KENNA SECURITY CASE STUDY

Charter Communications

Introduction

This case study of Charter Communications is based on an October 2019 survey of Kenna Security customers by TechValidate, a 3rd-party research service.

> “We needed a way to prioritize vulns because we have too many to work on traditionally.”

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Kenna Security:

- Vulnerability management challenges they experienced that led them to implement the Kenna Security Platform:
  - Inefficiencies in vulnerability remediation

Use Case

The key features and functionalities of Kenna Security that the surveyed company uses:

- Approaches used to prioritize vulnerabilities prior to Kenna:
  - Use rating system from scanner
- How they evaluate the success of their Kenna Security platform implementation:
  - Kenna risk score reduction
  - Reduction in vulnerability investigation time
  - Reduction in reporting time
- Kenna’s primary advantage(s) over other vulnerability management platforms:
  - Kenna goes beyond basic risk scoring and tells them what they need to fix first
  - Kenna provides meaningful and actionable data for remediation (remediation intelligence)
  - Kenna is updated continuously with real-time information
  - Kenna includes multiple threat intel feeds (eliminating the need for subscription)
  - Kenna’s cloud platform scales elastically to virtually any organization size

Results

The surveyed company achieved the following results with Kenna Security:

- Reduction of time spent on the following activities, since using Kenna:
  - Time spent on Vulnerability Investigation: over 50%
  - Time spent on remediation: over 10%
  - Time spent on reporting: over 75%

Company Profile

Company:
Charter Communications

Company Size:
Fortune 500

Industry:
Telecommunications Services

About Kenna.VM

Cisco Vulnerability Management (formerly Kenna.VM) offers an effective, efficient way to reduce your risk profile using risk-based prioritization powered by data science. Rely on it to ID the vulnerabilities that put you at the greatest risk, create a self-service environment for remediation teams, set intelligent SLAs based on your risk tolerance, compare your risk posture against industry peers, deliver clear reports with intuitive metrics, and more.

Learn More:

Cisco Vulnerability Management

Source: Robert Reinhold, IT Security Engineer, Charter Communications

Research by TechValidate by SurveyMonkey

✓ Validated Published: Oct. 15, 2019 TVID: D3D-35C-A57