KENNA SECURITY CASE STUDY

State & Local Government

Introduction

This case study of a state & local government is based on a November 2018 survey of Kenna Security customers by TechValidate, a 3rd-party research service. The profiled organization asked to have their name blinded to protect their confidentiality.

Challenges

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

- Security challenges experienced that led to implementing the Kenna Security Platform:
  - Too many vulnerabilities with no way to effectively prioritize
  - High volume of security data lacking context for decision making
- Previously used the following to prioritize vulnerability scan data:
  - Spreadsheets

Use Case

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

- Has been actively using the Kenna Security Platform for 9-12 months.
- Kenna Security Platform features most important to them when evaluating competitive or alternative solutions:
  - Data science-based risk scoring methodology
  - “Off the shelf” integrations with a wide range of security data sources

Results

The surveyed organization achieved the following results with Kenna Security:

- Most important security challenges the Kenna Security Platform has helped solve:
  - Addressing vulnerabilities that pose the greatest risk to their environment

Organization Profile

The organization featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Organization Size:
State & Local

Industry:
Government

About Cisco Vulnerability Management

Kenna is a software-as-a-service Risk and Vulnerability Intelligence platform that accurately measures risk and prioritizes remediation efforts before an attacker can exploit an organization’s weaknesses. Kenna automates the correlation of vulnerability data, threat data, and 0-day data, analyzing security vulnerabilities against active Internet breaches so that InfoSec teams can prioritize remediations and report on their overall risk posture.

Learn More:

Cisco Vulnerability Management

Source: TechValidate survey of a State & Local Government

Validated Published: Nov. 11, 2018 TVID: 219-064-934

Research by TechValidate by SurveyMonkey