Payken

API Penetration Test

Customer-Facing Document

Submission Date: February 5, 2026

Executive Summary

Rapid7 Consulting conducted an API penetration test for Payken between January 21 and January 23, 2026. This test was designed to provide Payken with an independent, point-in-time assessment of API vulnerabilities from the perspective of a malicious actor in accordance with Center for Internet Security (CIS) Controls and National Institute of Standards and Technology (NIST) guidelines.

Assessment Threat Synopsis

The following chart provides a summary of Payken's threat ratings:

Critical	High	Moderate	Low	Informational
0	0	0	2	1

During the analysis phase, Rapid7 evaluated Payken's security posture in the areas of:

- **Network Security:** Rapid7 evaluated the network’s security controls by testing Service Management, Encryption and Privacy, Admission Control, Authorization Control, and Patch Management.
- **Susceptibility to Brute-Force Attack:** Rapid7 evaluated if login portals can be brute-forced by testing User Accounts, User Passwords, Service Enumeration, and Service Passwords.
- **Internal Prevention and Monitoring:** Rapid7 evaluated how internal networks prevent and monitor intrusions by testing the Logging, Auditing, Intrusion Detection, and Threat Response.
- **Open-Source Intelligence Gathering:** Rapid7 evaluated how much Open-Source Intelligence (OSINT) is available by assessing User Accounts, Metadata, Social Networks, and Search Engines.

Threat Ranking Methodology

Rapid7 testing and vulnerability threat rankings are aligned to industry-proven NIST 800-30 threat rankings methodology. The following section outlines the NIST-based scoring methodology applied to the assessment findings:

Impact

		Informational	Low	Moderate	High	Critical
Likelihood	**High**	Informational	Low	Moderate	High	Critical
	Moderate	Informational	Low	Moderate	Moderate	High
	Low	Informational	Low	Low	Moderate	Moderate

Table 1: Threat Likelihood and Impact

Threat Likelihood

- **High:** A malicious actor is highly likely to initiate the threat event.
- **Moderate:** A malicious actor is somewhat likely to initiate the threat event.
- **Low:** A malicious actor is unlikely to initiate the threat event.

Threat Impact

- **Critical:** The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **High:** The threat event could be expected to have severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **Moderate:** The threat event could be expected to have serious adverse effects on organizational operations, assets, individuals, and other organizations.
- **Low:** The threat event could be expected to have limited adverse effects on organizational operations, assets, individuals, and other organizations.
- **Informational:** The threat event could be expected to have negligible effects on organizational operations, assets, individuals, and other organizations.

Level of Risk

- **Critical:** The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **High:** The threat event could be expected to have severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **Moderate:** The threat event could be expected to have serious adverse effects on organizational operations, assets, individuals, and other organizations.
- **Low:** The threat event could be expected to have limited adverse effects on organizational operations, assets, individuals, and other organizations.
- **Informational:** The threat event could be expected to have negligible effects on organizational operations, assets, individuals, and other organizations.

Note: See NIST's comprehensive methodology for more information:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Rapid7 Reporting Methodology

A Rapid7 report represents a 'snapshot' of the security posture of Payken's environment at a point-in-time. Rapid7 uses the NIST 800-30 threat ranking methodology, which enables Rapid7 to determine the impact, likelihood, and level of risk that a threat has to an organization.

Rapid7 provides the following within each assessment report:

- An Executive Summary with an assessment synopsis, high-level scope, testing constraints, and an assessment data section to provide an overview of what was performed during testing.
- An Assessment Findings section where the top five key findings and recommendations are called out to provide action items for remediation.
- An Assessment Storyboard to show the repeatable steps, the chained attacks, and to tell the story of what malicious actor could do when leveraging attack vectors.
- Finding sections with repeatable validation steps, recommendations, and remediation resources and references.

Rapid7 provides this report to Payken, who can use it as a plan to structure and track remediation efforts. Once Payken completes their remediation effort, Rapid7 can return for a remediation validation.