SOC2 vs ISO 27k Penetration Test

The main objective of a penetration test is to **enhance a company's security practices**.

Phases

		SOC2	ISO 27k
Planning & Preparation	Completing and signing the Scope of Work and Rules of Engagement	X	X
Mapping	Spidering, Fuzzing, Information Leakage, Authentication Determination and Username Harvesting	X	X
	Executing ping sweeps looking for additional servers not listed in the SoW, banner grabbing, smtp enumeration and executing techniques to try penetrating into targets (at the website or host level)		X
Vulnerability Testing	Session Attacks Discovery (Tracking, Fixation), Command Injection, File Inclusion, Directory Traversal, SQL Injection, XSS Test and HTML Injection	X	X
Exploitation (Optional*)	XSS, BeEF, AJAX, API Attacks, Data Attacks, CSRF, Logic Attacks and automated exploits		X
Reporting	Report includes Executive Summary, Introduction, Methodology, Findings, Recommendations and Network Level Scan	X	X

Important Notes:

- **SOC2** sprints usually take 3 weeks;, **ISO 27k** sprints usually take 4 weeks
- Customer can choose between testing within business hours (8-5pm PST) or outside business hours (5pm-8am PST)
- Customer can choose testing for their production or testing environment (we recommend production environment)
- Maximum of **2 websites and 1 API included for SOC2**, and the related servers to the websites/domains and the API
- **No restrictions** in the amount of websites, APIs and servers **for ISO 27k**