# XeneX SOCaaS

With over 12 years of experience and focus on Security Operations Center as a Service (SOCaaS), XeneX delivers a unique cybersecurity solution and unparalleled 7/24/365 SOC experience.

XeneX's software development team continues to extend the capabilities of XeneX platform. A leading industry platform, XeneX integrates several cybersecurity tools to achieve a single pane of glass of cybersecurity for the enterprise.

XeneX security analysts receive extensive training on the XeneX platform and must complete certification before joining the SOC team.


XENEX

SOC-AS-A-SERVICE

People, Process, Technology.

# Highlights

## *Network Scans*

These scans are used to identify vulnerabilities in network devices, such as routers, switches, and firewalls. They typically involve scanning for open ports, checking for known vulnerabilities in the software running on these devices, and assessing the configuration of the devices.

## *Web Application Scans*

These scans are used to identify vulnerabilities in web applications, such as SQL injection or cross-site scripting (XSS) vulnerabilities. They typically involve sending requests to the application to identify vulnerabilities in the input validation or output encoding mechanisms.

## *Cloud Environment Scans*

These scans are used to identify vulnerabilities in cloud environments, such as misconfigured permissions or insecure storage configurations. They typically involve scanning the cloud environment for known vulnerabilities in the software and configuration of the cloud resources.

## *Security Configuration Assessment*

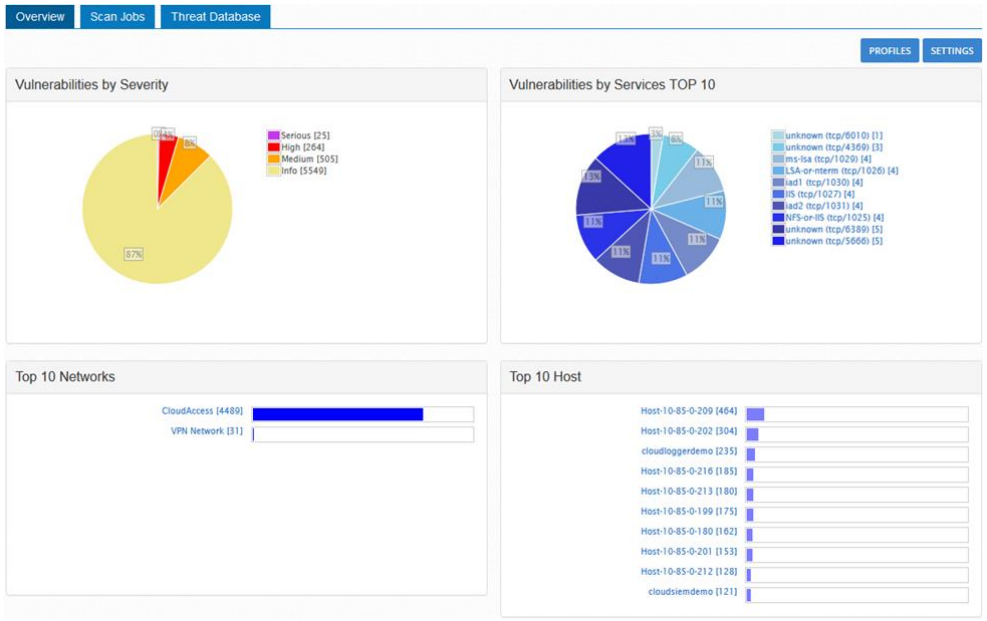
With this automated solution, XeneX quickly and effectively addresses security configuration issues.  This service eliminates the need for manual and time-consuming assessments that were historically performed by security staff. XeneX includes a set of policies based on the CIS benchmarks, a well-established standard for host hardening.

# XeneX Vulnerability Scan

A vulnerability scan is a type of security testing that is used to identify potential weaknesses in a system or network. It is typically performed using automated tools that scan the system or network for known vulnerabilities, such as missing software patches or configuration errors.

The objective of a vulnerability scan is to identify potential vulnerabilities before they can be exploited by attackers. By identifying and remedying these vulnerabilities proactively, organizations can reduce the risk of a successful attack and minimize the impact of any security incidents that do occur.

After a vulnerability scan is complete, a report is generated that outlines the vulnerabilities that were identified and provides recommendations for remediation. It's important to note that vulnerability scanning is just one component of a comprehensive security program and should be used in conjunction with other security measures, such as penetration testing and ongoing security monitoring.



# Our Vision

Continuously invest in technology, people and process improvements to deliver the most comprehensive cybersecurity technology platform and world-class white glove service for incident management.  To be the leading SOCaaS, protecting our partners and customers, and helping them achieve their cybersecurity goals.

# Contact Us


12121 Wilshire Blvd.

Suite 1111

Los Angeles, CA  90025

877-550-2568

info@xenexSOC.com

www.xenexSOC.com


XENEX

SOC-as-a-Service

People, Process, Technology.