VECTRA®

Vectra security assessment

Vectra® offers a complimentary service for Cognito® customers to identify opportunities to improve their security posture and identify compliance gaps. As part of this assessment, you will have access to expanded Cognito capabilities at no additional charge.

The Vectra security assessment gives you access to our dedicated team of experts, who will customize a set of prioritized recommendations to help you manage and reduce risk. Each expert will extend the know-how of your team with expertise gained across hundreds of Vectra deployments and from experiences securing some of the world's most sensitive assets. Your Vectra expert will sit side-by-side with you to empower your team to interpret business and compliance requirements into actionable Cognito results.

WHAT TO EXPECT FROM YOUR VECTRA SECURITY ASSESSMENT

- **Identify** security gaps
- **Categorize** compliance holes
- **Prioritized** recommendations customized for your environment

Your assessment service will require access to the relevant areas of your network and will run for three weeks in order to produce the best results.

Please contact vsa@vectra.ai to sign up for your complimentary assessment.

Standard checklist items included in your Vectra security assessment are shown in the table below.

VECTRA SECURITY ASSESSMENT

RDP exposed to the Internet	The Microsoft Remote Desktop Protocol is a target for attackers that can give them full control of network-connected devices. Over the years, a steady stream of vulnerabilities providing remote code execution and privilege escalation have surfaced, including BlueKeep. This service should not be exposed to the Internet.
SMB exposed to the Internet	Server Message Block (SMB) is an application-layer protocol that provides shared access to files, printers, and serial ports to devices on a network. SMB is a complex protocol with many known vulnerabilities, including EternalBlue, the exploit that enables the spread of WannaCry, NotPetya and other devastating ransomware attacks. This service should not be exposed to the internet.
Identify SMBv1 activity	SMBv1 is over 30 years old. Microsoft writes in a blog titled “Stop using SMB1” that “it was designed for a world that no longer exists. A world without malicious actors.” From anonymous NTLM logins to man-in-the-middle to EternalBlue, having this enabled on your network opens a broad spectrum of attacker exploits.
Identify TLS 1.0 and TLS 1.1 activity	TLS 1.0 is no longer PCI-DSS compliant. And Google, Apple, Microsoft and Mozilla have all announced that both TLS 1.0 and TLS 1.1 will be deprecated by early 2020 due to security vulnerabilities.
Use of telnet and unencrypted FTP	Telnet and FTP were not designed as secure protocols and, among other security issues, they pass credentials in the clear and are thus vulnerable to sniffing attacks. Upgrades to SSH and FTPS/SFTP are recommended to improve security posture.
Directly accessible IPMI/iDRAC	IPMI and iDRAC are lights-out management protocols critical to managing data centers at scale. Attractive targets for attackers, they provide sub-OS access to the baseboard management controller and often share common passwords that are embedded in scripts. It is important that access to the management networks that expose these services is carefully controlled, typically via a jump server.
NetBIOS and LLMNR usage	Both protocols are used to resolve hostnames on local networks, especially where DNS is not available. While enabled by default in Windows, both are susceptible to attacks and should be disabled if possible.
Unencrypted web administration activity	Access to directories and files common to web administration of common web applications over HTTP.
Unauthorized cloud storage usage	Identify all systems that access cloud storage – Dropbox, Box, Google Drive, iCloud, OneDrive – in violation of corporate policy.

VECTRA®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai