Cyber Exposure Diagnostic

Scoping Questionnaire

About

This document serves to provide:

- A brief overview of the scoping process
- Enable efficient collection of the required inputs for adequate scoping

For the Cyber Exposure Diagnostic (CED) services that you have recently ordered from Vodafone Business.

1. Scoping Process

Scoping a CED requires an understanding of the network and endpoint composition, which will help drive the appropriate level of coverage for CED analysis. For the network, this consists of capturing and analysing internet bound traffic. For the endpoints, focus is across both non-Windows e.g. Linux, Mac, etc. and windows operating systems

For the engagement, Accenture Security will provide the components for network and endpoint data collection. The equipment will be provided to all prioritised locations (e.g., in the case of multiple data centres, office locations, campus, etc.). Of primary concern, Accenture Security will perform a level of due-diligence to help ensure that the requirements of the equipment are well understood and addressed from the onset, which will help avoid complications during the execution of CED activities. This includes items such as firewall configuration, physical racking and power requirements, and network tap needs. Accenture Security will also configure as much of the systems in advance, where possible – for this, Internet Protocol (IP) addresses are required (e.g., "plug-and-play").

High-level scope – check all that apply:

System components	Number of in scope components
Endpoint & User	[Insert approximate number of endpoints]
Network	[Insert approximate number of network egress/ingress points]

1.1. Endpoint

The endpoint scope is determined by the number of endpoints (workstations and servers) to be included in the CED. Accenture Security utilises custom endpoint collection scripts for data collection

Endpoint Information Required including the table below):

- Are the following allowed Access outbound
    - Port 22 YES ☐ NO ☐
    - Port 443 YES ☐ NO ☐
- What is the deployment tool for enterprise software (SCCM, GPO, PDQ)?
- What, if any AV/EDR products are installed?
    - Who is the vendor?
    - Is there a Whitelist file/exclude folder?
- Who provides endpoint support, and would they be able to test and run CED scripts?

Please provide the following endpoint-specific information:

Endpoint Type (by Operating System)	Version(s)	Count Workstations	Count Servers
Windows [kernel 6.1 and newer] Windows 7 SP1 Windows Server 2008 R2 Windows Server 2012 R2 Windows 8.1 Windows 10 Windows 10 (Anniversary Edition)			
GNU / Linux Red Hat Enterprise Linux 6, 7 (x64) CENTOS 6.3 (and newer), 7 (x64) Ubuntu 14.04 (and newer) (x64) AWS Linux (x64)			
Mac OS (10.9 and newer)			
Other			

1.2. Network

The network scope is established as the complete accountability for all internet traffic, commonly referred to as so-called 'North / South' traffic. This could include all locations including data centers, offices, regional offices, and operations hubs. The goal is to capture and analyze all traffic sourced from the network in a manner that ensures any malicious communication is captured and identified.

Network Information Required including table below:

- Number of egress connections (internet links)
- Size or capacity (bandwidth) of each connection
- Utilisation of each connection, nominal usage and peak usage, on average
- Are there any Span/Tap limitations?
- Media type (copper vs fibre) to connect to ESX host from tap port?
- Who Provides network support?
- Please supply their contact information.
- Please provide a Network Diagram showing network ranges and connectivity in general, if available.

Please provide the following information per location:

Egress Point / Connection Description	Location	Size (Mb)	Utilization (average, peak)	Media Type

1.3. VM Hosting

VMWare Hosting Information Required including the table below:

- Does ESX host have 12 CPUs available in ESX for network sensor? – YES ☐ NO ☐
- Does ESX host have 64GB of memory Available in ESX for network sensor? – YES ☐ NO ☐
- Does ESX host have 2TB of Disk space Free on datastore for network sensor? – YES ☐ NO ☐
- Does ESX host have 2 Network ports?
    - Admin shared network port for access – YES ☐ NO ☐
    - Dedicated network port for network capture – YES ☐ NO ☐
    - Size or capacity (bandwidth) of each connection – NIC1: _____ NIC2:_____

Please provide the following information per ESX host:

ESXI Host	CPU	Memory	Network interfaces	Disk Space

In collaboration with

accenture

www.vodafone.com/business