

# Infrastructure Requirements The Platform™ 4.2

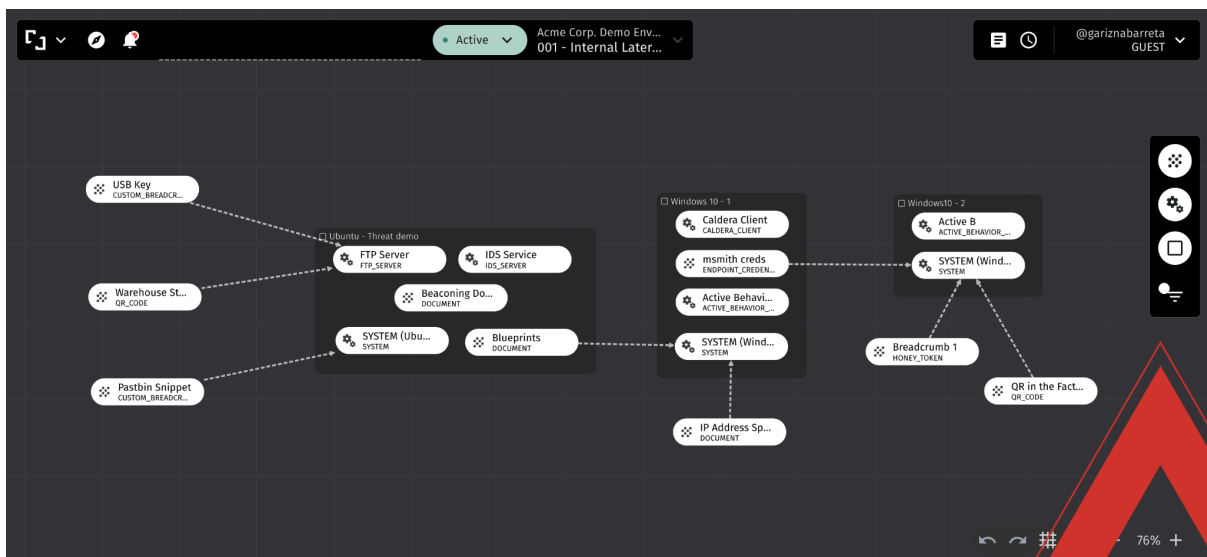


# Table of Contents

<b><u>Introduction</u></b>	<b><u>3</u></b>
<b><u>Understanding the Architecture</u></b>	<b><u>4</u></b>
<b><u>General On-Premises Requirements</u></b>	<b><u>5</u></b>
<b><u>Cloud-Specific Requirements</u></b>	<b><u>6</u></b>

# Introduction

Fortune 500 companies and government agencies trust CounterCraft to proactively defend against cyber threats and simplify their cybersecurity journey. The Platform is a leading deception-powered threat intelligence platform built to address the attacks that bypass organizations' security parameters.



Key features of CounterCraft Cyber Deception Platform include:

## Attack Graph

**The Attack Graph offers a relational approach to managing campaigns**, allowing users to effortlessly monitor the associated architecture and immediately uncover critical attacks. This intuitive interface offers meaningful context and clear visibility into the adversary's activities, all accessible from a single console.

## Data Explorer

**A feature that allows users to analyze and interpret the data** collected during a deployed campaign. It provides a centralized interface for viewing event logs, running advanced queries, and filtering data to identify attacker behavior and TTPs.

## Incidents

An incident represents a **structured collection of interactions, referred to as events, that are tied to the activities of a Threat Actor.**






## Integrations

CounterCraft offers a wide range of integrations for customers to leverage. These **integrations enable seamless data flow, incident response, and enhanced threat detection**, giving users a powerful toolkit for cybersecurity operations.



# General On-Premises Requirements






Internet connectivity is required during the installation of The Platform's components (Director, Tenant, Relay Node and Hosts).

On-Premises					
Component	vCPU	Memory (GB)	Hard Disk (GB)	Operating Systems	Networking
Director 	4	16	100	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on 443 port</li><li>· Outbound connections to the Tenant ports: 8123 / 7070</li></ul>
Tenant 	8	32	400	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections from the Director on ports: 8123 / 7070</li><li>· Outbound connections to Relay Node on ports: 7080 / 7070</li></ul>
Relay Node 	2	4	20	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections from the Tenant on ports: 7080 / 7070</li><li>· Inbound connections from the Deception Host on ports: 636 / 6514</li></ul>
Host (Linux) 	4	4	20	<ul style="list-style-type: none"><li>· Deception Hosts support Ubuntu versions 18.04, 20.04, 22.04, and 24.04; Debian 10 limited to 'SYSTEM and CUSTOM' services; Red Hat Enterprise Linux versions greater than 7.4, 8 and 9; CentOS 7 (versions 7.3 and above), 8 and 9, and limited telemetry for Linux ARM v7 devices, primarily routers.</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on whichever ports you want to expose as deception services</li><li>· Outbound connections to the Relay Node on ports: 636 / 6514</li></ul>
Host (Windows) <sup>1</sup> 	4	4	70	<ul style="list-style-type: none"><li>· Deception Hosts support a range of Windows desktop (XP, 7, 8, 10, 11) and server (2012, 2016, 2019, 2022) operating systems.</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on whichever ports you want to expose as deception services</li><li>· Outbound connections to the Relay Node on ports: 636 / 6514</li></ul>

<sup>1</sup> A Windows Deception Host cannot be instrumented if the Secure Boot is enabled. You can check if it's enabled using the command `Confirm-SecureBootUEFI`. If the result is False, or an error message, you can continue. If the result is True, you must deactivate the Secure Boot.







# Cloud-Specific Requirements

Internet connectivity is required during the installation of The Platform's components (Director and Tenant).

aws						
Component	Instance Type	Family	vCPU	Memory	Operating Systems	Networking
Director 	m7a.xlarge	M7a	4	16GB	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on 443 port</li><li>· Outbound connections to the Tenant ports: 8123 / 7070</li></ul>
Tenant 	m7a.2xlarge	M7a	8	32GB	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections from the Director on ports: 8123 / 7070</li><li>· Outbound connections to Relay Node on ports: 7080 / 7070</li></ul>
Relay Node 	m7a.large	M7a	2	8GB	<ul style="list-style-type: none"><li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li><li>· CentOS: Version 9 (CentOS Stream)</li><li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections from the Tenant on ports: 7080 / 7070</li><li>· Inbound connections from the Deception Host on ports: 636 / 6514</li></ul>
Host (Linux) 	m7a.large	M7a	2	8GB	<ul style="list-style-type: none"><li>· Ubuntu versions 18.04, 20.04, 22.04, and 24.04; Debian 10 limited to 'SYSTEM and CUSTOM' services; Red Hat Enterprise Linux versions greater than 7.4, 8 and 9; CentOS 7 (versions 7.3 and above), 8 and 9, and limited telemetry for Linux ARM v7 devices, primarily routers.</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on whichever ports you want to expose as deception services</li><li>· Outbound connections to the Relay Node on ports: 636 / 6514</li></ul>
Host (Windows) <sup>2</sup> 	m7a.xlarge	M7a	4	16GB	<ul style="list-style-type: none"><li>· The platform supports a range of Windows desktop (XP, 7, 8, 10, 11) and server (2012, 2016, 2019, 2022) operating systems.</li></ul>	<ul style="list-style-type: none"><li>· Inbound connections on whichever ports you want to expose as deception services</li><li>· Outbound connections to the Relay Node on ports: 636 / 6514</li></ul>







<sup>2</sup> A Windows Deception Host cannot be instrumented if the Secure Boot is enabled. You can check if it's enabled using the command Confirm-SecureBootUEFI. If the result is False, or an error message, you can continue. If the result is True, you must deactivate the Secure Boot.

Internet connectivity is required during the installation of The Platform's components (Director and Tenant).

						
Component	Instance Type	Family	vCPU	Memory	Operating Systems	Networking
Director 	Standard_D4as_v6 ▾	Dasv6 ▾	4	16GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on 443 port</li> <li>· Outbound connections to the Tenant ports: 8123 / 7070</li> </ul>
Tenant 	Standard_D8as_v6 ▾	Dasv6 ▾	8	32GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections from the Director on ports: 8123 / 7070</li> <li>· Outbound connections to Relay Node on ports: 7080 / 7070</li> </ul>
Relay Node 	Standard_D2as_v6 ▾	Dasv6 ▾	2	8GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 20.04, 22.04, and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections from the Tenant on ports: 7080 / 7070</li> <li>· Inbound connections from the Deception Host on ports: 636 / 6514</li> </ul>
Host (Linux) 	Standard_D2as_v6 ▾	Dasv6 ▾	2	8GB	<ul style="list-style-type: none"> <li>· Ubuntu versions 18.04, 20.04, 22.04, and 24.04; Debian 10 limited to 'SYSTEM and CUSTOM' services; Red Hat Enterprise Linux versions greater than 7.4, 8 and 9; CentOS 7 (versions 7.3 and above), 8 and 9, and limited telemetry for Linux ARM v7 devices, primarily routers.</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on whichever ports you want to expose as deception services</li> <li>· Outbound connections to the Relay Node on ports: 636 / 6514</li> </ul>
Host (Windows) <sup>3</sup> 	Standard_D4as_v6 ▾	Dasv6 ▾	4	16GB	<ul style="list-style-type: none"> <li>· The platform supports a range of Windows desktop (XP, 7, 8, 10, 11) and server (2012, 2016, 2019, 2022) operating systems.</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on whichever ports you want to expose as deception services</li> <li>· Outbound connections to the Relay Node on ports: 636 / 6514</li> </ul>

<sup>3</sup> A Windows Deception Host cannot be instrumented if the Secure Boot is enabled. You can check if it's enabled using the command Confirm-SecureBootUEFI. If the result is False, or an error message, you can continue. If the result is True, you must deactivate the Secure Boot.

Internet connectivity is required during the installation of The Platform's components (Director and Tenant).

 Google Cloud Platform						
Component	Instance Type	Family	vCPU	Memory	Operating Systems	Networking
Director 	n2d-standard-4 ▾	N2D ▾	4	16GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 22.04 and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on 443 port</li> <li>· Outbound connections to the Tenant ports: 8123 / 7070</li> </ul>
Tenant 	n2d-standard-8 ▾	N2D ▾	8	32GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 22.04 and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections from the Director on ports: 8123 / 7070</li> <li>· Outbound connections to Relay Node on ports: 7080 / 7070</li> </ul>
Relay Node 	n2d-standard-2 ▾	N2D ▾	2	8GB	<ul style="list-style-type: none"> <li>· Ubuntu: Versions 22.04 and 24.04</li> <li>· CentOS: Version 9 (CentOS Stream)</li> <li>· Red Hat Enterprise Linux (RHEL): Versions 8 and 9</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections from the Tenant on ports: 7080 / 7070</li> <li>· Inbound connections from the Deception Host on ports: 636 / 6514</li> </ul>
Host (Linux) 	n2d-standard-2 ▾	N2D ▾	2	8GB	<ul style="list-style-type: none"> <li>· Ubuntu versions 22.04 and 24.04; Debian 10 limited to 'SYSTEM and CUSTOM' services; Red Hat Enterprise Linux versions greater than 7.4, 8 and 9; CentOS 7 (versions 7.3 and above), 8 and 9, and limited telemetry for Linux ARM v7 devices, primarily routers.</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on whichever ports you want to expose as deception services</li> <li>· Outbound connections to the Relay Node on ports: 636 / 6514</li> </ul>
Host (Windows) <sup>4</sup> 	n2d-standard-4 ▾	N2D ▾	4	16GB	<ul style="list-style-type: none"> <li>· The platform supports a range of Windows desktop (XP, 7, 8, 10, 11) and server (2012, 2016, 2019, 2022) operating systems.</li> </ul>	<ul style="list-style-type: none"> <li>· Inbound connections on whichever ports you want to expose as deception services</li> <li>· Outbound connections to the Relay Node on ports: 636 / 6514</li> </ul>

<sup>4</sup> A Windows Deception Host cannot be instrumented if the Secure Boot is enabled. You can check if it's enabled using the command Confirm-SecureBootUEFI. If the result is False, or an error message, you can continue. If the result is True, you must deactivate the Secure Boot.