CounterCraft

Specific. Actionable.
Threat Intelligence
Powered by Deception.

CounterCraft Technical Requirements

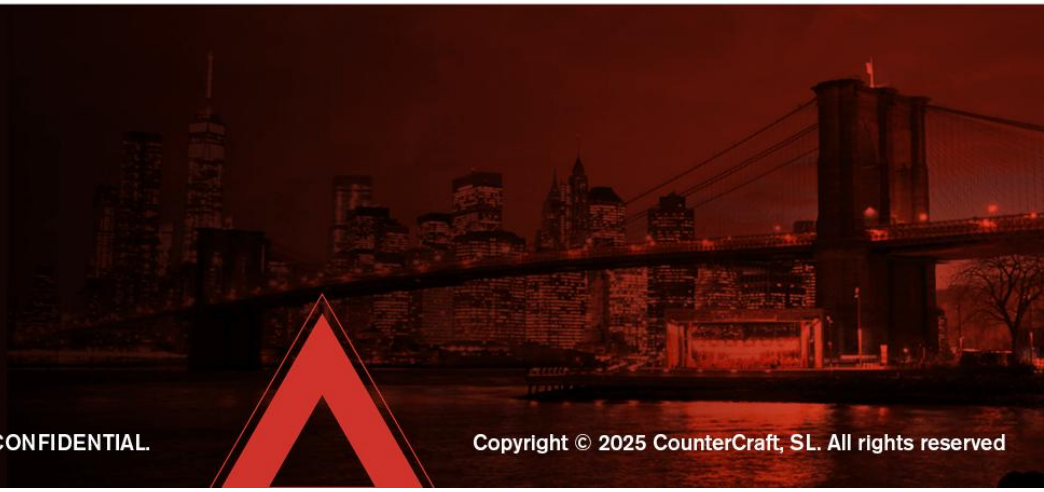


Table of Contents

Product Requirements

The product requirements for the CounterCraft Platform are as follows:

- Licenses valid for at least **3 years** from delivery.
- Includes **5 host licenses** and **1 central management platform**.
- Must support **updates and product support** during the license period.
- Includes **consultation (40h)** and **training (40 academic hours)** for at least 5 users

Functional Capabilities

The CounterCraft Platform supports all of the following functional capabilities:

Creation of **fake services** with breadcrumb trails (e.g., fake documents).

The CounterCraft Platform allows the creation and deployment of a wide range of fake services with breadcrumbs trails. The services can be drawn from a pool of software packages available out-of-the-box or custom software packages to adapt to the required deception deployment.

Full OS simulation, scriptable environments, and content generation.

The CounterCraft allows the use of fully functional real OS devices from a wide range of distributions for both 64bit, 32-bit and ARM architecture.

These environments can be managed using scripts to interact with the onboard RESTFul API.

Content generation is a road-mapped function due for release at the end of 2025.

Integration with **Active Directory**, **Exchange**, & monitoring capabilities

The CounterCraft allows integration with Active Directory either through the seeding of deception resources or the creation of deception instances for functionality and credibility within a deception environment.

Exchange can be included as a deception service.
Both scenarios provide extensive monitoring of any adversary interaction with them.

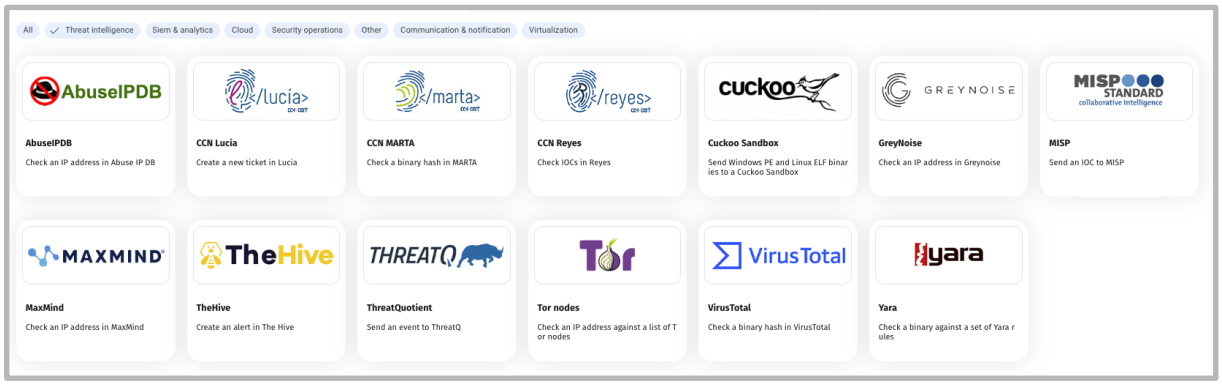
Compatibility with **SIEM tools**: Elastic Search, SPLUNK, ArcSight.

The CounterCraft Platform has out-of-the-box connectors with ArcSight, SPLUNK and Elastic Search SIEM solutions. Additionally the EQL search syntax used by Elastic stack is also employed within the Platform for advanced search capabilities.

Integration with **sandboxing and threat intel platforms**: Cuckoo / MISP

The CounterCraft Platform supports the export of event data to MISP.

With reference to sandboxing solutions, the Countercraft Platform automatically captures any binary that is executed within the deception environment. These binaries can be piped into a Cuckoo sandbox.

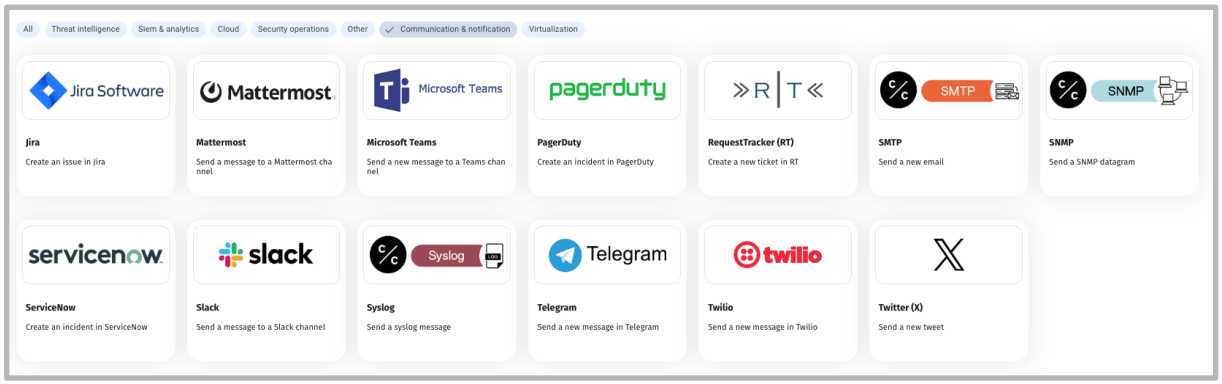


Threat Intel and sandboxing solutions supported by CounterCraft

Messaging platform integration: Mattermost, Telegram, Teams, Slack.

The CounterCraft Platform support all the following messaging systems:

- Mattermost
- Slack
- Microsoft Teams
- Telegram



Messaging, Comms and Notification solutions support by CounterCraft

API integration with **Jira** and **TheHive**.

The CounterCraft supports direct integration with both Jira and The Hive through the management console, and allows creation of tickets automatically based on trigger events. Both solutions can also be integrated using the onboard RESTful API.

MITRE CALDERA simulation and ATT&CK TTP mapping.

The MITRE ATT&CK TTP framework is fully integrated into the CounterCraft Platform, both for Enterprise and ICS. All event data is cross-referenced against both frameworks and all matching events are tagged with the corresponding TTP.

Supported Services & OS

Services

The CounterCraft Platform supports, but is not limited to, the use the following protocols and software packages within deception environments,:

- SMB
- RDP
- Exchange OWA
- VPNs
- Git
- Apache
- SMTP
- SNMP
- POP3/IMAP
- SYSLOG
- HTTP/HTTPS

Operating Systems

The CounterCraft Platform supports but is not limited to the use of the following operating systems with deception deployments:

- Windows Server 2012-2022
- Windows XP, 7-11
- Ubuntu 18.04–22.04 LTS.

Management & Security

Centralized web-based management with SSL

The CounterCraft Platform is managed using a web based management interface hosted by the centralized Director server. This acts as an access broker and is responsible for all AAA actions, providing full roll-based access control (RBAC) to the interface. Access to the web interface is protected using SSL.

Alerting via email, customizable by user.

Alerts from the CounterCraft Platform can be sent by email, among other channels, and the configuration of both the email service and content is fully customisable.

Logging of administrative changes.

All administrative changes within the platform are logged, as are user access sessions and any configuration changes within the deception campaigns.

Three user roles: Administrator, Architect, Observer

Firstly, there are two global user roles available within the platform:

Admin - a role that is used to create Tenants and to perform all system administration tasks within the platform, such as user creation or software upgrades. The Admin user has access to all tenants.

Standard - a role that is applied to all other users. Standard users are assigned the tenants that they can interact with by the Admin user.

Secondly, within a Tenant a user may be assigned as an Tenant Architect or Tenant Standard:

Tenant Architect - The role of the Tenant Architect role is to create and manage tenant deception architecture and campaign deployment. Tenant Architects are responsible for installing tenant Deception Support Nodes and for creating Campaigns.

Tenant Standard - Standard users are simply permitted to interact with the Campaigns created by the Tenant Architect..

Finally for every campaign there are Managers, Analysts and Guests:

Manager - Managers are able to assign other user accounts to be Managers, Operators or Guests within their Campaign.

Analyst - The primary responsibility of this role is the day-to-day operation of a Campaign. Analysts are able to configure all entities within a Campaign (that has previously been created by an Architect).

Guest - Guests are a Read Only role, primarily for auditing purposes.

Non-functional Requirements

Logging of deception network and admin interface changes.

All deception network and admin interface changes are logged by the Countercraft Platform.

Marking of products with manufacturer info

The CounterCraft Platform is a software only solution, In terms of provision and deployment it is provided as a licensed download from CounterCraft to be installed on customer hardware. As such the requirement for marking is not applicable.

Within the software itself, version information is provided and further details of the Software Bill of Materials (SBOM) is available on request.

Delivery via email; keys/licenses sent encrypted.

As previously mentioned the delivery of the software for installation is via a licensed software download. The license key to enable and verify the download is provided by email.

Advance notice required for physical/electronic delivery.

Advance notice for electronic delivery of the license key can be provided. Typically the license key is sent to the customer representative identified during the procurement process.

Includes **handover documentation** and **quality control** procedures.

Handover documentation is provided, typically in the form Technical design Document. This is supplemented by additional documentation according to customer requirements.

The typical onboarding process is outlined in the enclosed document:

Deception Infrastructure Setup and Deployment Activities.pdf

Minimum requirements for deploying the CounterCraft are outlined in the following enclosed document:

Infrastructure Requirements — The Platform 4.2.pdf