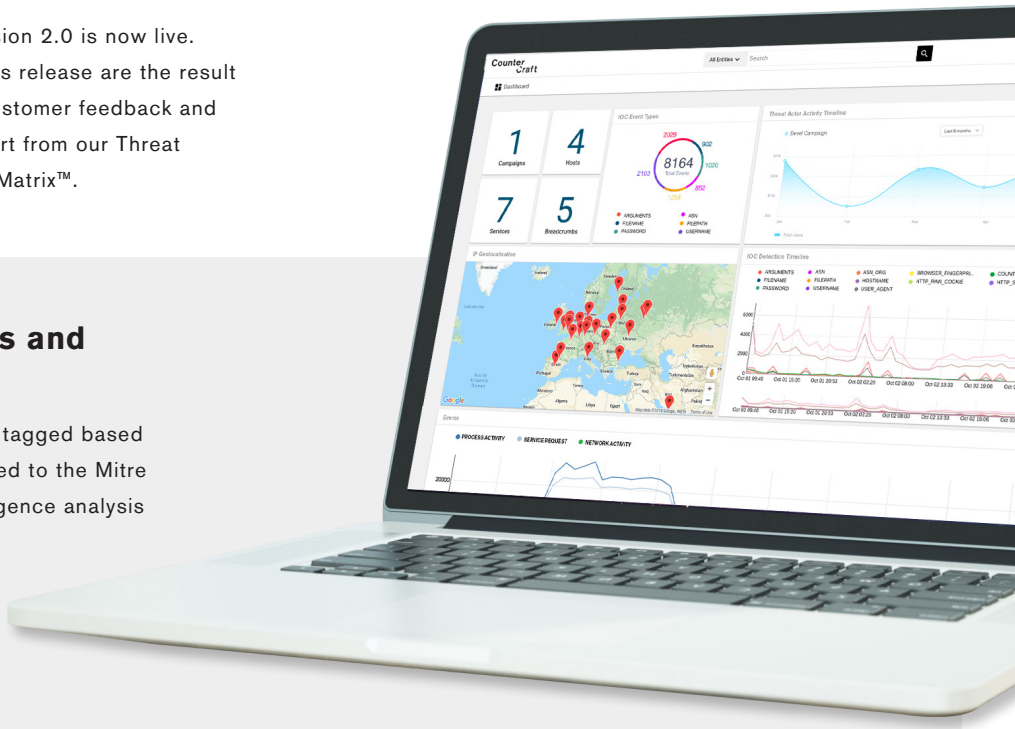
Technical Memo: What's new on CounterCraft 2.0 release

We're pleased to announce that CounterCraft version 2.0 is now live. New features and functionality improvements in this release are the result of significant investment in UX and UI based on customer feedback and market demand for simplicity, and outstanding effort from our Threat Intelligence team to integrate the MITRE ATT&CK Matrix™.



Adversary Behaviour Analysis and Threat-Actor Identification

Allows malicious activity to be identified and tagged based on known IOCs and TTPs. This data is mapped to the Mitre ATT&CK Matrix™, providing new threat intelligence analysis and facilitating threat hunting teams with the power to identify adversaries and their modus operandi.

Streamlined for Simplicity

Management and deployment processes have also undergone improvement. The design and deployment workflow has been simplified and streamlined in response to feedback from our customers. The aim is to ensure that the design, deployment and management of deception environments is intuitive and efficient for experienced users, and to reduce the amount of training required for those new to the task.

Better Monitoring and Metrics

This release includes stage one of implementation the Prometheus monitoring engine to provide powerful metrics and host keepalives to monitor the health of the deception environment. Deception environment visibility is radically improved, and support for heartbeats and health checks is enhanced.

Metrics are displayed on the CounterCraft console, with certain metrics now displayed directly on the CounterCraft dashboard.

Synthetic Email Scenarios

Advanced machine learning to enable the creation of email content for deception email accounts. CounterCraft has developed a powerful tool to create believable email streams to populate fake email accounts when using Office 365 or local email accounts within a campaign.

Kubernetes Support

Full installation is now possible in a Kubernetes environment; this automates deployment, scalability and management of containerized applications.

Keyword Watch

This new feature allows a user to identify high value events and objects using custom defined keywords. The keywords are patterns that the system will automatically try to match on new events and objects. They are typically used to reveal suspicious activity – for example, a login attempt using a password that suggests the presence of insider knowledge. Each keyword can be assigned a score to numerically represent its importance to the campaign. The keyword score will be affixed to all events/objects that match the keyword, and can be used to filter information.

Updated Agent Features

A number of enhancements have been made to agent features:

- Random agent-process naming
- Network support for Windows
- Full agent cloaking in Windows and Linux
- Agent-based event grouping
- Web-based remote shell
- NTLM proxy support

HSS

HSS is a Communication Protocol that connects Deception Host to the Deception Support Node and allows direct execution of commands, file transfers, the creation of interactive shells. It is also used to gather metrics from hosts.

Role-Based Login

Users can now be assigned permissions on an individual campaign basis. This allows basic multi-tenancy for campaigns managed by the same Deception Director.

New Assets Available. Enriched Scope of Deception Assets.

Office 365 Spear-Phishing

Using the new O365 integration it is possible to create false accounts and use them to respond to spear phishing attacks. The logs from the O365 account are gathered by the CounterCraft Deception Director to provide a view of how the account is being hijacked by the adversary, and how it is being abused; this type of insight has never been made available before.

Wireless networks

It is now possible to include wireless networks in the deception environment, opening up a multitude of possibilities to monitor who is connecting to the wireless network, what credentials they are using and what their motivation is for doing so.

Office 365, Google Docs and Active directory

These services and platform types have been added to increase the breadth of possibilities for the Deception Architect.

Third Party System Integration

MISP Threat Sharing

Office 365

siem

MISP

The CounterCraft Deception Director allows direct integration with a MISP instance, allowing threat intelligence gathered from a deception campaign to be shared either within an enterprise or among the wider threat intelligence community.

Microsoft Office 365

Use the new Office 365 plugin from the Deception Director to create deception user accounts and monitor activity. Accounts can be populated with seemingly real email content using CounterCraft machine learning-based tools.

SIEM & Orchestration Platforms

Thanks to the improved RESTful API, integration with SIEM and orchestration platforms is even easier.