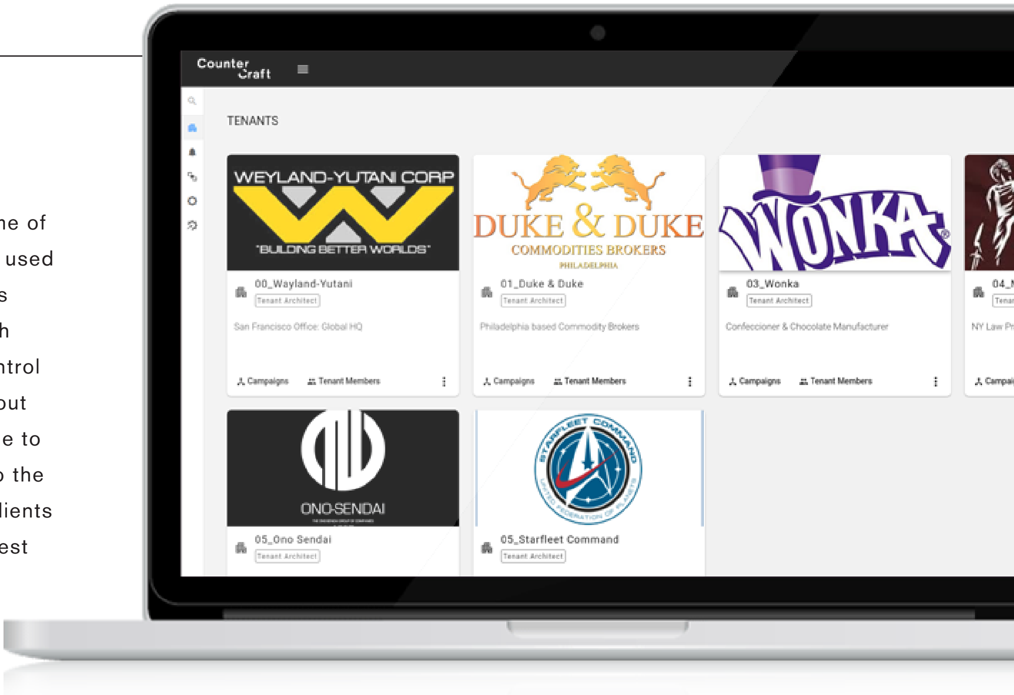
Technical Memo:

Improving threat intelligence creation to enhance active defense with CounterCraft 2.8

Introduction

CounterCraft's latest release features substantive improvements in our cyber deception platform, some of which are unique in the industry and already being used by important clients. Building on the improvements in version 2.7, which included a full integration with MITRE Shield and ATT&CK as well as endpoint control and WiFi and IoT capabilities, version 2.8 is all about improving the threat intelligence customers are able to gather. The release includes a definitive solution to the issue of multi-tenancy, allowing work on multiple clients from a single console, a long-awaited feature request based on direct feedback from our clients.



An Unprecedented Level of Deception Credibility

CounterCraft version 2.8 includes the introduction of our revolutionary new ActiveBehavior (Human Interaction Simulator) technology. This provides a huge leap forward for deception host credibility by solving the age-old "Marie Celeste" problem (a lack of real users and user history data) of how to make it look like the deception hosts are in current use - like a real production system. This gives an unprecedented level of realism and allows clients to include user activity across different deception hosts.

With ActiveBehavior, create activity in your deception environment such as:

- ✓ **Periodic logins**
- ✓ **Command executions**
- ✓ **Web browsing**

All designed to look exactly like regular human behavior, and all automated. This exciting new technology was based on an extensive funded research program. Compatible with Linux and Windows, ActiveBehavior is already being deployed in deception systems, and its level of effectiveness is wowing both our team and our clients.

Delivering Cutting Edge Ways to Gather Threat Intel

CounterCraft 2.8 hones in on bringing value to customers, focusing this time around on bringing bigger, more powerful tools to the threat intelligence table. The following new features in this version are designed to enhance efficiency and intelligence analysis:

ActiveBehavior

Making deception environments ultra realistic

The launch of a proprietary technology that allows deception environments to remain fresh and tempting to threat actors, making deception environments ultra realistic.

ActiveBehavior is a huge leap forward for deception host credibility, making environments look like real, active production systems. This unprecedented level of realism is incredibly effective.

Full Multi-Tenancy

Allowing multiple client deployments from a single console with full segregation

Now, CounterCraft can be deployed for multiple clients from a single console. This fully featured multi-tenant solution was one of the most frequent asks from CounterCraft clients, and we've designed the definitive solution with version 2.8. The creation of the new "Super Architect" role allows a user to control various clients' deployments of the platform while maintaining full segregation between tenants managed from the same deception director.

Easy File Browsing in Deception Hosts

Making on-the-fly management simple

The introduction of a new file browser in version 2.8 represents a huge leap forward in host management for the platform. The new graphic file browser allows full interaction with the deception host's file system. Users can access anything from uploads to downloads to file edits. As the file browser session is hidden it also allows real-time adversary interactions - monitoring exfiltration or binary uploads and even changing the modifications. This new feature makes deploying and refreshing breadcrumbs, as well as making on-the-fly changes to the system really simple.

Enhanced Performance via EQL

Create complex searches and improve analysis

The new EQL feature in version 2.8 allows the creation of a standardised query language for events. This feature is integrated into the platform's Data Explorer, allowing it to execute complex searches and improving analysis capabilities. With EQL, clients can easily identify specific events and patterns, giving threat intelligence performance a huge boost.

Performance Boost

Optimising backend processes to boost performance

CounterCraft is constantly streamlining its platform and to improve performance. This enhancement allows for streamlined agent communications and backend processing. With new event field name normalization, the event filtering language becomes even more powerful, allowing users to push blacklists to the agent in a much easier, more efficient manner. Events can also be handled without checking against hundreds of regexes.

New Third-Party System Integrations

GREY NOISE

CounterCraft now allows direct integration with Grey Noise's internet-scanning technology, allowing users to contextualize alerts and track threats. The integration allows data collected in the deception environment to be sent to your Grey Noise account via the CounterCraft API.

GitHub

Integrate GitHub, the world's largest development platform, into your deception environments. This feature allows users to create a public GitHub Gists as breadcrumbs. Gist is an easy method to share snippets or excerpts of data with others. A Gist breadcrumb can be a string of code, a bash script or some other small piece of data.

PROXMOX

The CounterCraft integration with ProxMox allows users to manage their QEMU and LXC virtual machines directly from the CounterCraft console. The PROXMOX integration allows users to start, stop, pause resume, shutdown and reboot virtual machines. It also allows snapshots and rollbacks to streamline VM management.

About CounterCraft

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time.

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time. Learn more at **www.countercraftsec.com**.

Download our latest documents at

🌐 countercraftsec.com

or if you prefer contact us at

✉ craft@countercraftsec.com