Technical Memo:

Making advanced active defense even easier to use and increasing coverage with CounterCraft 2.9

CounterCraft

Introduction

CounterCraft's latest release features a bundle of improvements made with our clients in mind. This version builds on the strides made with version 2.8, which included the introduction of ActiveBehavior, an industry-first human interaction simulator. Version 2.9 is all about refining different aspects of our platform to make them easier to deploy and more user friendly, from further integration EQL to new solutions specific to specialized sectors.

Major Improvements in Ease of Use

CounterCraft version 2.9 is simpler than ever to deploy. From day one, the changes in 2.9 will drastically cut the configuration time necessary to get the Cyber Deception Platform up and running. One of the standout changes is the ability to automatically create notifications for new services—it is no longer necessary to do this manually. This frees up your team's valuable time without reducing the effectiveness of the platform. Other ease of use improvements in the new version include:

- **Automatic rules created for new services**
- **Simplified daisy-chaining, directly from the console (select licenses only)**
- **Windows screenshot capability**

The new version also features increased coverage for RHEL 7 and 8 and also new access to SUSE Linux.

Focusing on the Bottom Line : Faster Threat Intel

CounterCraft 2.9 focuses on the end goal: deception that brings in accurate, real-time threat intelligence. Version 2.9 packages up several powerful enhancements that add up to faster (and, as always, ultra credible) threat intelligence for your organization.

EQL Everywhere

Industry standard EQL query language available everywhere

EQL, or Endgame Query Language, is now present in every aspect of the platform. Rules now use EQL syntax, and the Data Explorer event search feature works with EQL as well.

This means improved searchability and ease-of-use with a more flexible language for generating threat intelligence.

MITRE ATT&CK Upgrade

Running the latest version of MITRE since the day of launch

CounterCraft is the only deception vendor to run a true integration of MITRE ATT&CK in the platform. We had integrated the latest version of MITRE on the day of launch. The improvements now include compatibility with containers and Google Workspaces.

Automated Rule Creation

A huge time saver

We've automated the creation of rules, a key component of any deception campaign. Rules are now automatically added for new services, which means users will get automatic notifications for service specific adversary activity.

Air-gapped Installs and Daisy Chaining configs

A solution for military customers

For customers with a military license, these two upgrades are extremely useful. The new air-gapped installer allows deployment in unconnected network environments. Just define the environment, download and install! The install bundle contains all the software required to install the Deception Director, the Deception Support Node, and all supported services for the chosen operating systems.

ActiveBehavior Personas

Further evolution of this revolutionary feature

Our last update featured the unveiling of ActiveBehavior, the Human Interaction Simulator. Now, in 2.9, it continues to evolve. The latest version of ActiveBehavior features new user personas for even greater credibility, a new configuration option menu within the service menu, and select personas with different behavior patterns to enhance believability.

New Third-Party Support & Updates

Microsoft Active Directory

The new CounterCraft Active Directory update allows users to include Zero-Logon attack detection. This new addition means Active Directory features within CounterCraft are even more useful.

SUCURI Real People. Real Security.

CounterCraft now provides new support for Sucuri's website security scanner. This allows monitoring of activity registered by the Sucuri security tool for protecting events and users within WordPress environments.

SUSE

The new SUSE support on the CounterCraft platform allows CounterCraft to communicate with the industry's most adaptable Linux operating system, providing world first deception support for SUSE users.

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.

Their award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload. Founded in 2015, CounterCraft is present in London, New York, New York and Madrid, with R&D in San Sebastian, Spain. Learn more at **www.countercraftsec.com**.

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com