Cyber Deception Tech Brief: SOC & Incident Responders

Providing detailed threat data for SOC Engineers & front-line incident response teams

Actionable specific data from highly instrumented Deception Assets

The CounterCraft Cyber Deception Platform provides detailed telemetry from highly instrumented deception assets, that provides a step-by-step insight into every action that is taken by a threat actor in the deception environment.

Extract detailed information about every move and tactic that is being used as part of the attack campaign by using Deception Hosts – real machines loaded with advanced hidden agents.

Each area within this decoy server or High-Interaction Honeypot is capable of collecting highly detailed granular data and information in real-time. The telemetry gathered across the deception environment is exported via the Deception Support Nodes to the Deception Director™.

The Console provides visualization of everything that is being managed by the Deception Director™, enabling detailed engineering and analyst views through to high-level abstracted Deception Campaigns, Attack Trees, Threat Analysis, Intelligence and CISO reporting.

Data value from Deception Assets for the SOC team

The integrity of the data gathered from deception assets either within the classical enterprise perimeter or beyond through to the cloud, or Social Media platforms, provides specific first-hand data on adversaries who are directly attacking what they think are your real enterprise production assets.

This detail enables Incident Responders and Engineers to view exactly the specific paths that are being taken through a server, and what malware or exfiltration tools are being used as part of the attacker Tactics, Techniques and Procedures (TTPs).

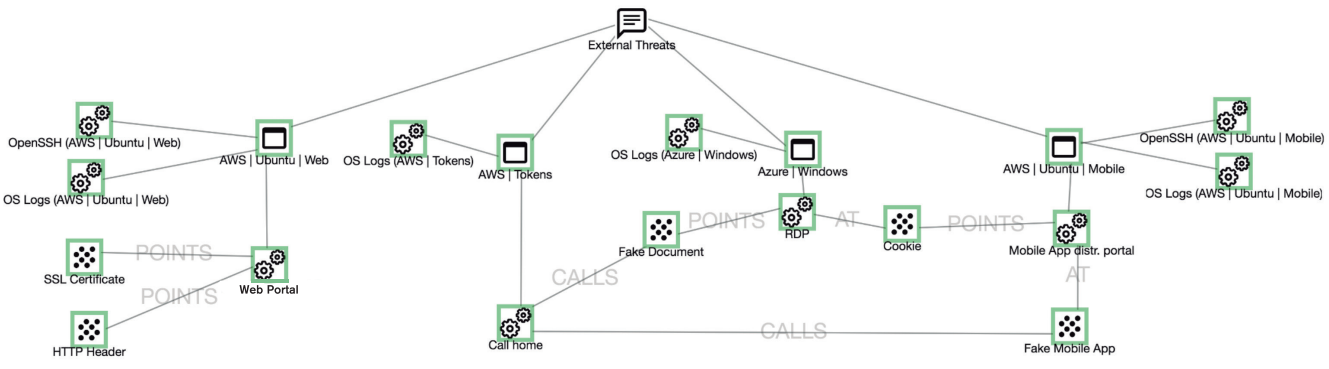
As the attacker moves within the deception environment, steered by the Deception Logic™ that has been created within the Deception Director, multiple Deception Assets may be orchestrated, each delivering detailed data that can be viewed at different layers of abstraction.

Powerful Deception Monitoring

Each Deception Host has a cloaked agent that provides deep insight from the kernel up of all activities being performed. The agent monitors processes, files, file systems, memory, network indicators and other key aspects and records every action being taken.

Deception Services and other deception material that are run or placed on the server to make it appear as real as possible, are also monitored.

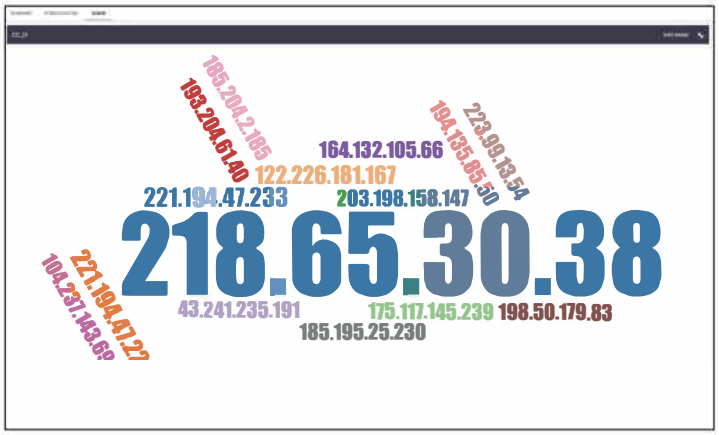
The granularity of detail can be adjusted to suit the specific environment, and critically all data and information is passed unfiltered to the Deception Director™, where it is stored and processed according to specific criteria.



Data Visualisation

The attacker Course of Action and threat telemetry from the distributed deception assets is viewed from the Deception Director™ Console, providing different levels of interpretation and abstraction to match the needs of specific operational personnel and roles. The data is useful for operational, tactical and strategic analysis purposes.

The Cyber Deception Platform enables threat data enrichment through mechanisms such as geolocation, YARA signatures, VirusTotal and the fusion of associated information that is relevant to building a Threat Intelligence understanding of what is being uncovered by the deception environment – the interplay between attack campaigns and deception campaigns, driven by the Deception Logic™.



About Deception Assets

CounterCraft enables the deployment of assets to engage with determined adversaries as they pass through different stages of an Attack Lifecycle – from Reconnaissance through to Maintenance – all contained within a controlled deception environment.

All assets are orchestrated by Deception Logic™ that provides the ability to engage adversaries automatically using a rule based expert system; to gather first hand Threat Intelligence and steer them away from real assets whilst gathering highly detailed telemetry on their TTPs.

The Cyber Deception Platform allows creation of scalable components from simple SSL Certificate “Breadcrumbs” to full scale Containerised synthetic environments populated with Deception Personas, false documents and transactions that provide a true depth to deliver an Authentic Deception experience to the attacker.

To achieve the scale required by the most demanding complex organisations the architecture deploys Deception Support Nodes that provide efficient workload and segmentation capabilities acting as intermediaries between Assets and the Deception Director™ & Console.

Interoperability and Integration with SOC tools

SOC environments, Engineers and Analysts use many different tools to perform their OpSec activities. The Deception Director™ provides an extensive range of features and a full RESTful API to enable deception environment data and information to be exported in real-time or batch mode to these external systems.

The base data and information models that enable sharing Indicators of Compromise (IOCs) or Indicators of Attack (IOA) are contained within the Deception Director™ architecture.

Options such as CSV, JSON, OpenIOC, STIX 2.0 and MISP are currently supported and are used to communicate deception based Cyber Threat Information & Intelligence to SIEM (Security Information & Event Management) and Threat Management & Analysis platforms.

Learn more about CounterCraft deception

REGISTER FOR A TRIAL

craft@countercraftsec.com

© 2018 CounterCraft. All rights reserved.