CounterCraft Platform Brief: Deception Director™

Deploy targeted deception across the enterprise

Built to scale in the most demanding environments

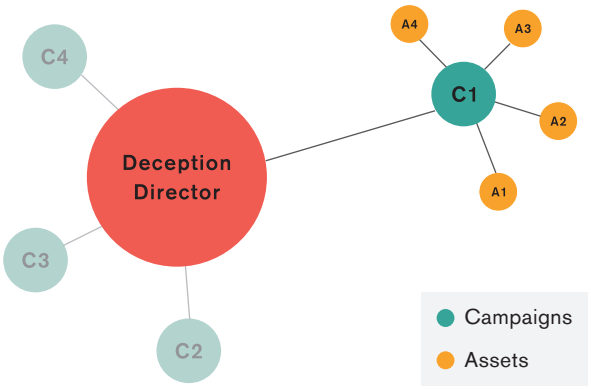
The CounterCraft Deception Director™ is the key component of the CounterCraft Cyber Deception Platform.

Modular architecture

To keep pace with the rapidly evolving world of Cyber Deception, the Deception Director™ has been developed with a modular architecture to allow rapid introduction of new features and capabilities.

New or enhanced product functionality can be created through specialized Capability Modules that comply with architecture plug-in standards. Modules can either have external interfaces from the Director where communication is required, e.g. STIX / OpenIOC for Threat Intelligence sharing or can purely operate within the Deception Director™.

This approach has delivered a fully featured, and scalable product that is successfully deployed in customer sites today.



Deception Director™ – delivering Threat Intelligence, Cyber Defence and Incident Response

Creating and sharing Threat Intelligence

The Deception Director™ product collects, collates and analyses real-time Threat actors and their behaviour within the deception environment. Engaging across the enterprise ICT estate also provides an Active Defence mechanism for the CISO, protecting information assets and disrupting attackers. The information gathered can be shared in machine-to-machine format to augment other enterprise security systems.

The Deception API Suite – designed for deep integration

A fully RESTful API is available for the Deception Director™. This innovative approach enables deep and detailed control of major Deception Director™ deception attributes. It also ensures that as Security Operations and Threat Intelligence centres evolve and scale the CounterCraft Cyber Deception Platform can provide functionality and information at a granular level to other platforms.

It responds to emerging architectures and initiatives such as the US Integrated Active Cyber Defence, and its adoption within the global Financial Services industry.

Integration and Interoperability

The Cyber Deception Platform is designed to be flexible; to adapt and integrate into the existing operational enterprise ICT. In the case of the Deception DirectorTM the most common requirement is to interact with Security & Information Event Management (SIEM) and Threat Management or Threat Intelligence systems. Standard mechanisms such as SysLog or OpenIOC are available and specific protocols can be added to suit custom installations.

Core features and functionality

The following areas create powerful deception orchestration, automated response, analytics and visualization aspects that are critical in support of Defensive Cyber Deception Operations (DecOps):

Console visualisation. The power of the Deception Director™ is its ability to reduce complexity. Different users need to visualise different data, from SOC operators and Incident Responders to Threat Analysts and Deception Planners. This is achieved through a rigorous approach to visualisation and levels of abstraction that are matched to particular job roles and environments.
Multiple enterprise users with specialist roles in security, architecture, deception planning and threat analysis can work at different task levels, including pooling knowledge if required to create the optimal deception environment and campaigns.

Deception Asset configuration. Context aware configuration screens guide users to create all aspects of the deception environment. Configuration stages provide a logical set of relationships between Deception Assets, and their placement within the enterprise ICT estate, establishing the interplay between operational and deception ICT.

Deception Logic™. At the heart of the Deception Director™ is the key ability to enable Deception Planners and Threat Analysts to rapidly build their deception models and approaches for intelligent interaction with adversaries. Both intelligence and hypothesis led cyber deception methodologies are supported by the logic constructs, to provide a broad range of choices that do not constrain the planners.
The level of abstraction is geared towards orchestrating the complete set of Deception Assets as simply as possible; to achieve defensive and threat intelligence gathering goals.
Multiple parallel Deception Campaigns can be built, and sections of logic can be easily re-used, improving the productivity of highly skilled cyber professionals.

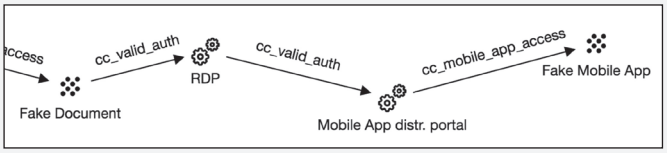
Automated Complex Defence Response. The Deception Director™ can respond automatically to an attack. The Deception Logic™ provides the conditional rule set that controls the specific actions - manipulating the deception environment in response to the adversary.
This approach enables an Informed Incident Response capability to be supported within the complete Cyber Deception Platform, and also link to external structures such as SIEMs.

Engagement Decision Engine™. Once the Deception Environment has been configured, the Deception Assets and the Deception Logic™ are deployed into the live environment, the interaction can begin. The interplay between attacker actions and defensive behaviour is orchestrated through the Deception Director™ running and overseeing the distributed Engagement Decision Engine™ capability across all of the Deception Assets.

Deception Event management & Alerting. In the live environment data is gathered from across the Deception Environment from the smallest deception artefacts through to complete complex systems built on fully instrumented Deception Hosts. All this detailed telemetry is sent to the Deception Director™ over SSH secured channels for complete visibility.

Collation and Correlation. To handle the volume and velocity of information being generated in large complex deception environments, the Deception Director™ uses powerful Collation and Correlation tools. These allow Deception Operations personnel to rapidly establish what is happening in their environment, and to decide quickly what actions need to be taken.

Attack Graphing. One critical technique for understanding and analysing the behaviour of a cyber attacker is through visualizing their progress and decisions using Attack Graphs. These live feed models provide defenders with immense insight into Tactics, Techniques, Tools and Procedures, and how the Deception Campaigns are impacting the attacker in their enterprise. Threat Analysts can use whichever approaches they prefer to perform complex Intrusion Analysis, and can more easily spot intrusion sets that may be used by multiple attackers, improving the defenders Situational Awareness.



Database infrastructure. The Deception Director™ utilizes powerful database constructs to handle the real-time and scaling requirements of the attack information that is generated by the deception assets. The database architecture is designed to obtain the best performance possible to enable data analysis and relevant collation and correlation for Threat Intelligence and Threat Analytics.

Learn more about CounterCraft deception

REGISTER FOR A TRIAL

craft@countercraftsec.com