CounterCraft Platform Brief: Deception Assets

Distributed high fidelity Enterprise Class deception

Business context is critical

Modern day enterprise ICT infrastructures, business applications and business processes, are evolving at a rapid pace. This makes it imperative that any attempt to create believable deceptions applies particular attention to the need to blend in with the expected operational landscape. Credibility is key.

CounterCraft offers a range of Deception Assets through its Breadcrumb Library, Deception Services and Deception Hosts. They are designed to be hidden in plain sight, and exist comfortably with standard IT Services Management tools and disciplines. This ensures that the fundamental ICT operations are not impacted through the deployment of deception technologies as part of an enhanced Enterprise Cyber Defence strategy.

The requirement to meet the, often disparate, business needs within large complex organisations is key to the CounterCraft approach; enabling Deception to be a natural defence approach which adds value to the organisation in protecting its valuable information assets.

Enterprise ICT – the major elements that influence Deception Asset decisions

The shift to “work anywhere - anytime” while maintaining access to critical organisational information assets and systems, and the growth in extended digital supply chains with multiple partners has taken its toll on classical enterprise security architectures and disciplines. The shift to the cloud is a good example of the blurring of the classic enterprise perimeter that would have marked the “edge” of the organisation to be protected.

Deception Assets must co-exist in these adapting environments, augmenting and mimicking the live operational assets, being attractive targets for adversaries to engage with and provide defenders with valuable Cyber-Counterintelligence to shape their countermeasures accordingly.

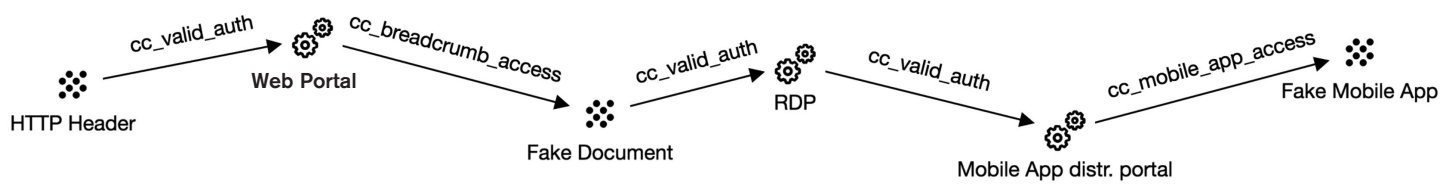
About Deception Assets

CounterCraft has developed an architectural approach that enables the seeding of assets to engage with determined adversaries as they pass through different stages of an Attack Lifecycle from Reconnaissance through to Maintenance where they aim to remain persistently in the Enterprise environment.

All of the assets are orchestrated by Deception Logic™ that provides the CISO with the ability to engage the adversaries automatically using a rule based expert system, gather first hand Threat Intelligence and steer them away from real assets whilst gathering high fidelity Digital trace information on their Tactics, Techniques and Procedures.

We provide 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 Deception Assets and the Deception Director™ & Console.



Assets Types

Breadcrumbs

These are considered to be small pieces of deception material that are only likely to be discovered or triggered by threat actors. The interaction often leads deeper into the deception environment, where more complex capability is deployed to engage and manipulate adversaries and build a more detailed knowledge of their complete agenda.

The Breadcrumbs are categorised into Passive and Active.

Examples of Passive Breadcrumbs would be SSL Certificates and distinct credentials, or pointers to a vulnerable web application, or PasteBin data. Active Breadcrumbs might be a Mobile App or Honey Tokens.

CounterCraft provides expert support and development tooling that is matched to the task. Customers are introduced to this as we work with them through the CounterCraft Deception Asset Studio™ programme that matches the Campaign design to their business requirements.

Breadcrumbs are designed to be deployed using industry standard tools such as Microsoft GPO and McAfee ePO platforms or through our Cyber Deception Platform Console.

The Console provides real-time visual monitoring, tracking and alerting of any adversarial engagement with a Breadcrumb and places it into the relevant Attack Tree and Deception Logic™ context.

Deception Hosts

CounterCraft has developed a growing range of capability that now encompass Windows Server, Linux, Routers, WiFi Access Points and Mobile Phones, that provide specific attack characteristics information and adversary engagement options. These are fully instrumented environments to enable deep technical inspection of adversary behavior through the Operating System stack. Secure telemetry ensures this information is passed through Deception Support Nodes to the Deception Director™ for processing and action.

Deception Services

These are more complex components in the Deception environment, designed to increase attacker “dwell time” in the synthetic world, enabling the enterprise defence team Threat & Intelligence Analysts to gather first hand knowledge of their adversaries and adjust cyber defence strategy and investments as a result.

Deception Services can be a range of common IT capabilities such as Office 365, Webservers, MySQL, Active Directory, GitHub repositories, specialised application servers such as those used in SWIFT banking infrastructure.

A critical aspect of our deployment flexibility is our exploitation of Containers in the creation of authentic deception assets. This enables us to benefit from the innovation and power in a rapidly evolving adjacent area to our own area of specialisation.

Many organisations have moved to deploying Virtualisation and are adopting a range of Cloud services and architectures. The Deception Services we create match this complex set of options, and can be matched to blend in with operational machines and service deployments. Deception Services can be deployed in bare metal OS mode (Linux / Windows), as Virtual Machines, in Private Cloud, Hybrid Cloud, Public Cloud, SaaS, PaaS, and IaaS, and Containers.

Deception Personas

Ensuring Deception environments are believable to an attacker requires a focus on building and maintaining strong fake credentials, individual identities and expected behaviour patterns from a normal ICT usage perspective. CounterCraft works collaboratively with customers during the Deception Asset Studio™ engagement process to develop and deliver appropriate Deception Personas.

Learn more about CounterCraft deception

REGISTER FOR A TRIAL

craft@countercraftsec.com