Deception 101

CounterCraft

Augment Enterprise Cyber Defence with advanced Cyber Deception Technologies

Organisations continue to face daily cyber attacks designed to disrupt their businesses or strategic missions by adversaries using an evolving set of Tactics, Techniques and Procedures (TTP).

Defenders continually feel that they are at a disadvantage as they need to protect their assets all the time in organisations which no longer have classical boundaries or perimeters, and who are adopting new technologies, business models and global partnership at a faster rate than ever before.

A new approach and way of thinking that is now being blended into classical cyber defence behaviour is to start to use Deception tools and techniques to protect important information assets and systems, and divert persistent adversaries to synthetic environments which engage to gather direct threat intelligence, keep them occupied and misdirect them through Deception Campaigns.

What can Deception do to defend across the Attack Lifecycle?

Although many principles of Deception have been applied in military and intelligence domains for many years it has only been applied within the enterprise space for the past few years as technology and understanding has grown to provide cyber defenders with a new capability.

If your organisation is new to the concept of Cyber Deception as an emerging component in an enterprise defence in depth strategy then we hope to introduce you to some of its value now.

To understand how cyber adversaries may behave, models that are termed Attack Lifecycles, have been developed to describe the stages that most attacks will go through to reach a goal, the most commonly referenced model being that originally developed by Lockheed Martin - the Cyber Kill Chain®.

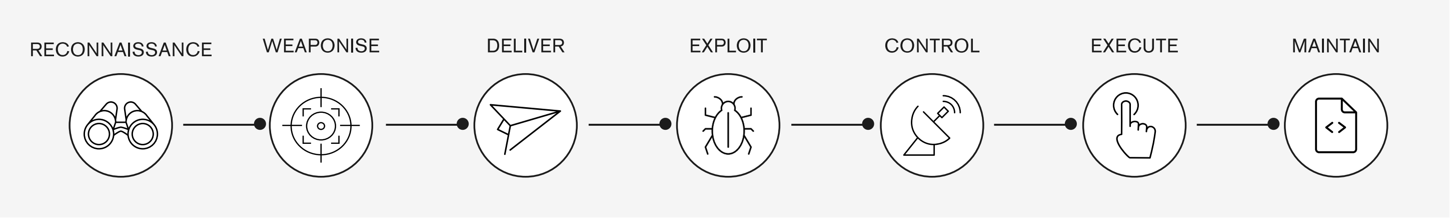
Using this model as a background we can describe how Deception thinking and technologies can really improve the ability of organisations to protect their information assets and business resilience. Below is the blend of stages and the potential Deception options that can be part of a relevant defender Course of Action (CoA).

The Defender Deception options were originally articulated by Mitre Corporation in a paper published in November 2013 looking to establish vocabulary that described cyber defence approaches in support of Cyber Resilience.

We can use the Kill Chain model interacting with Defender Deception methods to describe some of the ways that Deception can work through an Attack Lifecycle. We could have chosen the Mitre ATT&CK model which has more stages, or other models, but we feel that once you have the sense of any Attack Lifecycle then you can choose the specific models that resonate best with your particular environment and granularity of analysis.

The stages are labelled primarily from the attackers viewpoint:

Attack Stages



RECONNAISSANCE — WEAPONISE — DELIVER — EXPLOIT — CONTROL — EXECUTE — MAINTAIN

Defender Deception Options

PREVENT	DETER	DETER	DETER	DETER	DETER	DETER
IMPEDE	DECEIVE	DIVERT	DIVERT	DIVERT	DIVERT	DECEIVE
DIVERT		DECEIVE	DECEIVE	DECEIVE	DECEIVE	DETECT
DECEIVE				DETECT	DETECT	
DETECT					DEGRADE	
DEGRADE						
ANALYSE	**ANALYSE**	**ANALYSE**	**ANALYSE**	**ANALYSE**	**ANALYSE**	**ANALYSE**

CounterCraft

CounterCraft: **Full Deception enabled Defence**

✓ **PREVENT** ✓ **IMPEDE** ✓ **DETER** ✓ **DIVERT** ✓ **DECEIVE** ✓ **DETECT** ✓ **DEGRADE** ✓ **ANALYSE**

Critically you can see that at every stage, Analysis is a major outcome, which is the basis for good Cyber Threat Intelligence production.

Improve cyber defence using a Protect, Detect & Respond philosophy - how Deception helps.

As in many areas of life and business the Pareto principle appears to apply, and the world of Cyber security is no different. Through deploying standard enterprise security technology such as Firewalls, Anti-virus, Intrusion Detection & Intrusion Protection systems; adopting security controls such as CIS Top 20, ISO 27001; staff Security & awareness training; and maintaining good software patching disciplines it is likely that 80% of cyber attacks will be successfully mitigated.

Which leaves the 20% that aren't being mitigated for a range of reasons.

No matter how good the defenders get the over-riding issue is that organisations are made up of people, processes and technologies, all of which have vulnerabilities that can be exploited. So with the sheer scale and dynamics of modern organisations it is becoming apparent that if you have something of value - intellectual property, money, personal information, competitive advantage - then a motivated cyber adversary will have found a way to access your systems.

It could be argued that in the 21st Century our vulnerability landscape is increasing rather than diminishing due to the rate that software, the app economy, mobile devices and the rush to Digital Business Transformation causes quick semi-tested solutions to be deployed. There is a desperate need to minimise the impact this is having on information and cyber security.

Deception technologies and Deception Operations work on the principle that the adversary is either already in your enterprise, and is well hidden, or that they are making their way through the stages of an attack lifecycle - ***and critically that they also have vulnerabilities.***

Building an advantage through intelligent Deception

Improving knowledge of your adversaries ahead of any subsequent breach or cyber incident will give you as a defender the beginning of an advantage. The topic of Threat Intelligence and organisations in both the public and private sectors being providers, consumers and sharers has grown quite dramatically over the past 5 years. As this has happened there have been major moves to standardise language and processes related to how threat actors behave and can be categorised according to their visible Tactics, Techniques and Procedures.

Whilst this undoubtedly provides Chief Information Security Officers with better information that can be applied to evolving their organisational Situational Awareness, getting to a point of relevant, actionable Threat Intelligence has remained difficult to achieve - until now.

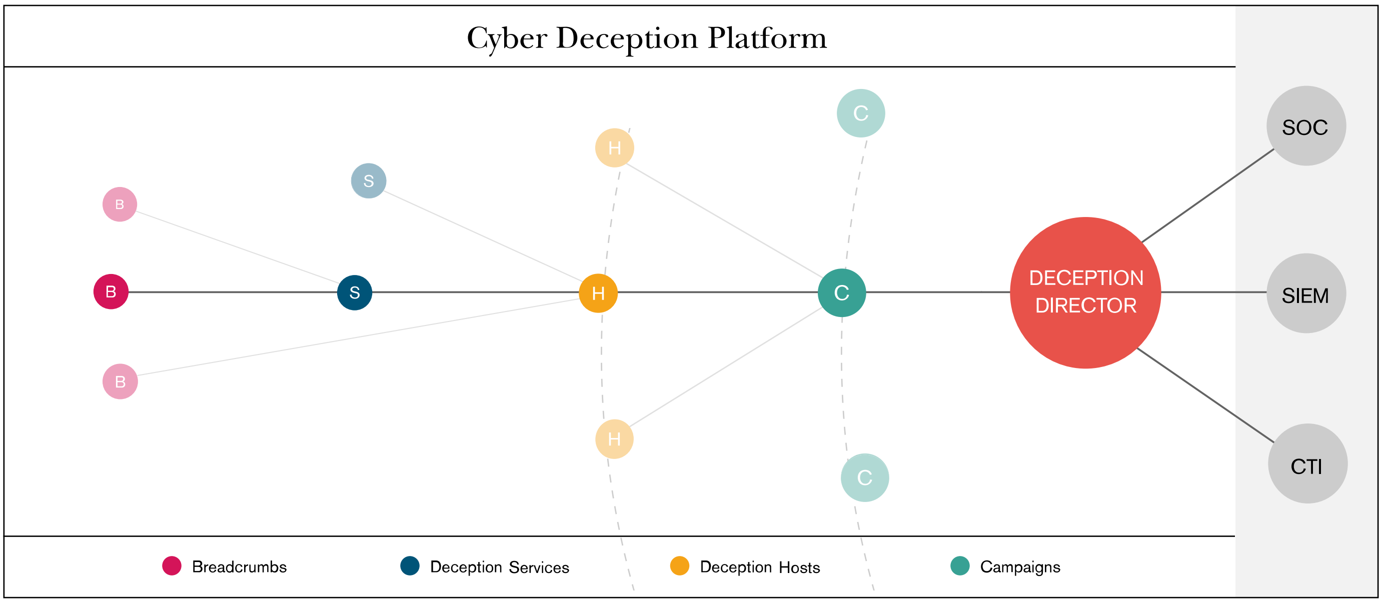
Deploying Deception assets across an enterprise all the way from remote internet based Cloud Services through to executive mobile devices, servers or even WiFi access points enables a business context specific 1st Party Threat Intelligence capability to be built, refreshed and acted upon in real-time.

The software based Deception assets are designed to blend in with the standard enterprise ICT environment, and are deployed intelligently as required by the nature of the enterprise cyber defence strategy and threat landscape. The assets, can be scaled to match the breadth and depth of a required deception layer, in effect offering an attractive and dynamic “attack surface” to engage multiple adversaries with targeted Deception Campaigns.

As adversaries engage with aspects of the deception environment, believing they are navigating the real enterprise, specific information is gathered by the assets through a combination of agentless and complex software Deception Agents™ at many levels, building a comprehensive activity trace record. This detail is gathered across a secure deception telemetry network embedded across the enterprise that is managed by Deception Support Nodes (DSN) feeding in to the CounterCraft Deception Director™.

From this central vantage point enterprise cyber defence personnel can both create and deploy Deception Campaigns as well as monitor in real-time the current visual status of ongoing campaigns and adversaries in different stages of an Attack Lifecycle.

Subsequent strategic and operational decisions can then be based on real evidence - before a breach, exfiltration of data or manipulation of critical business processes has occurred.



Why not consider using CounterCraft Deception Technologies and methods as a key part of your Enterprise Defence strategy?