SMOKESCREEN

Deception Defence Platform

SOLUTION DOCUMENT

Discover how Smokescreen's deception defense platform can enable you to build world-class threat detection and response capabilities.

Version: 210420

WHO ARE WE?

At Smokescreen, we use our deep insight into how apex hackers operate to build deception-based defenses that detect and stop post-breach attacks.

RECOGNITION & ACCOLADES

Gartner COOL VENDOR

"Smokescreen Technologies is cool because it uses a combination of machine learning and deception to detect cyberattacks that bypass the protection mechanisms in place."

SC MEDIA

5/5 STAR RATED DECEPTION PLATFORM

"IllusionBLACK accurately and efficiently detects targeted threats in real-time by deploying decoys across the kill-chain."

black hat

5/5 STAR RATED DECEPTION PLATFORM

Smokescreen is the only deception vendor that runs the 5-star rated training on deception at Black Hat USA

Gartner

TOP RATED IN VENDOR COMPARISON

"The only vendor that actively detects and counters attackers' measures to detect or bypass deceptions."

DSCI
PROMOTING DATA PROTECTION

RECOGNISED BY DSCI

Awarded the most innovative product of the year, 2016 and security product company of the year in 2017

INTRODUCING ILLUSIONBLACK

Smokescreen IllusionBLACK uses deception technology to blanket your network with decoys to detect targeted attacks involving reconnaissance, lateral movement, malware-less attacks, Man-in-the-Middle attacks, and ransomware, in real-time.

HOW DO WE HELP YOU?

PROBLEM	SOLUTION
Low Network Visibility With complex and vast networks, businesses have very little visibility behind their perimeter. This makes it extremely difficult to detect intrusions.	**Network and Endpoint Deception** Decoys and lures placed across the network detect intrusions giving you unparalleled visibility into malicious activities in your network.
Changing Attack Tactics Apex attackers constantly change their tools and tactics making signature and behavior-based detection ineffective. Thus businesses struggle with detecting APTs, zero-days, and new strains of malware.	**Attack Agnostic Detection** Deception technology does not rely on signatures or behavior to detect attacks. Any interaction with a decoy is suspicious making it effective in detecting attacks irrespective of tools or tactics used.
False Positives Traditional security solutions generate thousands of alerts leaving security teams overwhelmed. This leads to event fatigue, data paralysis, and missed alerts. The problem is pervasive. The attack at Target Corp was detected but no one noticed – it was lost in the noise.	**Higher Quality Alerts** By design, deception is a low false-positive solution. No one knows that decoys exist in the network/ Therefore, no legitimate user should be accessing a decoy. As a result, any interaction with a decoy is a high-confidence, high-fidelity indicator of a breach.

WHY ILLUSIONBLACK?

- Full kill-chain coverage as opposed to numerous point solutions.
- Offers a unique, customized defense against targeted threats.
- Able to detect malware-less attacks and internal fraudsters stealing data.
- Native integrations with leading security solutions for automated response.

HOW IT WORKS

IllusionBLACK creates decoys (fake systems) on the network that look like real servers hosting services – databases, web-servers, applications, file shares, etc. These decoys are deployed alongside your real assets in your datacenter. IllusionBLACK also creates fake credentials, cookies, processes and files that serve as lures for attackers and are deployed on your real endpoints.

For an attacker who has broken in, the decoys look as real a legitimate system. The moment they interact with a decoy, a silent alarm is raised while the systems collect information on the attacker's actions and intent. Automated response actions can also be taken using built-in isolation feature or though integrations with popular firewalls and EDRs.

WHAT DECOYS DO WE SUPPORT?

PERIMETER DECOYS

Internet-facing decoys that heuristically engage only with targeted threats against your organization while ignoring random Internet scans.

DECOY LURES

Dummy credentials injected on endpoints lure hackers when escalating privileges. They point to decoy systems and alert when used.

FILE DECOYS

Decoy files with custom content in various formats placed on high value target systems that trigger when a file is opened, accessed, copied, or deleted.

CLOUD DECOYS

Detect lateral movement in your AWS and Microsoft Azure cloud environments with decoys like web servers, databases, file servers, etc.

SPEAR-PHISHING DECOYS

Email decoys that engage with attackers attempting to mount social-engineering / spear-phishing attacks on high-value personnel.

NETWORK DECOYS

Decoys that look like server systems that host services like SSH servers, databases, file shares and more.

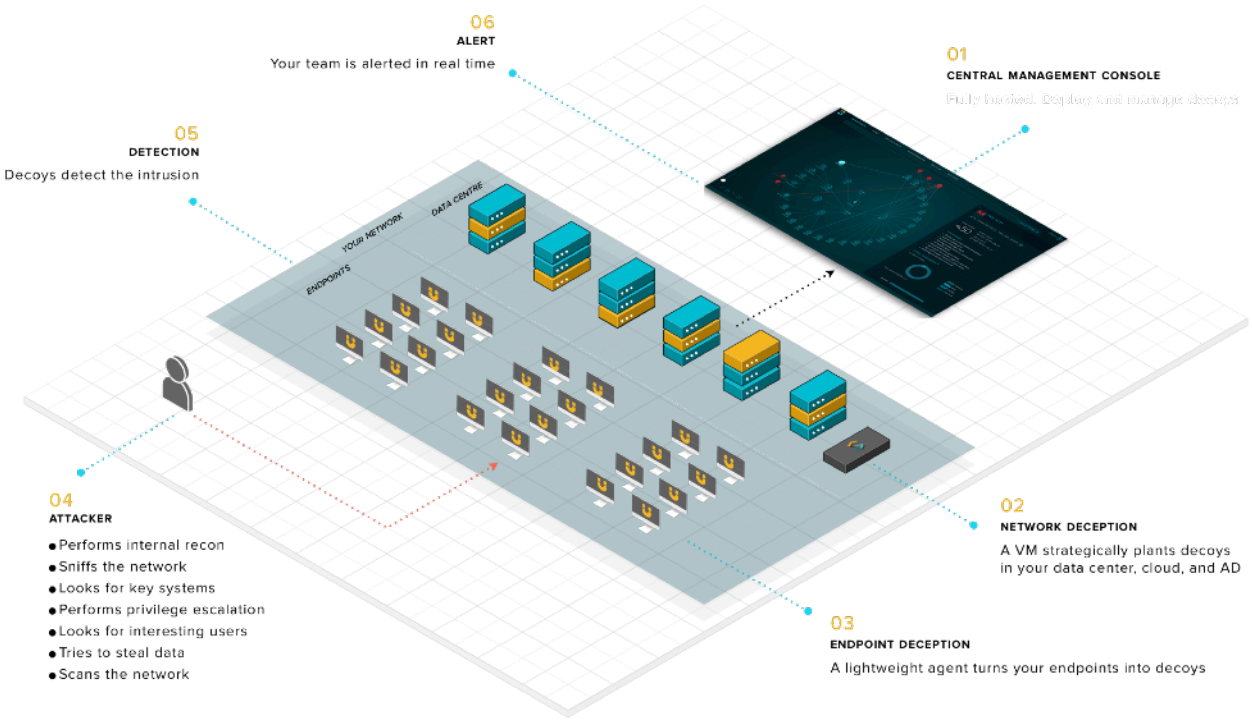
HIGH INTERACTION DECOYS

Decoys that mimic the interface and functionality of applications you use at your company, leading attackers to believe that they've broken in.

MITM DECOYS

Detect Man-in-the-Middle attacks for protocols like LLMNR, mDNS, and NBT-NS by identifying the spoofer.

ARCHITECTURE



COMPONENTS

01. Central Management Console

The CMC serves as the central point of management and analysis for the solution. All other appliances and agents connect to the CMC and all deployment and configuration is performed through it. All events are collected, analyzed and forwarded based on orchestrated rules. The CMC also provides a powerful UI dashboard for deep analysis of events.

02. Network Appliances

These are lightweight virtual appliances that are deployed in data centers and can create network decoys across multiple trunked VLANs. They also host multiple high interaction decoy virtual machines that lure attackers into believing that they are interacting with real systems in the environment.

03. Landmine Agents

These are software agents that are deployed on real endpoints (desktops/ laptops) in the network. They deploy fake credentials, decoy files, browser cookies, fake processes etc. on the endpoints.

About Smokescreen

At Smokescreen, we use our deep insight into how apex hackers operate to build deception based defenses.

Our deception platform, IllusionBLACK, is the industry's most advanced decoy technology — bringing military deception principles to the digital battlefield.

Smokescreen's solutions protect some of the most highly targeted organizations globally, including leading financial institutions, and Fortune 500 companies.

Email: kali@smokescreen.io
Phone: (+1)6032332838
Web: www.smokescreen.io