Choosing A Deception Platform

A COMPETITIVE COMPARISON

How to choose a deception platform.

When faced with numerous deception solutions, including simple scripts, open-source honeypots, and commercial systems, how do you decide what's ***actually effective*** against targeted attacks?

Read on to see how the options compare. When you're done, we're confident you'll see why Smokescreen's IllusionBLACK is far-and-away the most advanced and complete deception solution available.

Capability	Open-source honeypots	Other deception providers	Smokescreen's IllusionBLACK	Why it matters to you
Basic service emulation	✔	✔	✔	Decoys should speak basic protocols like HTTP, SSH and FTP that are heavily attacked. If your deception solution doesn't do this, look elsewhere.
Email alerts	✔	✔	✔	Deception systems should be able to alert the security team in real-time when a decoy is accessed. If the system cannot give you real-time alerts, you won't catch attackers when you need to most.
Regular updates		✔	✔	Attackers are not static. A well-designed deception solution receives regular updates and has a strong development roadmap. Ask about ours.
No false positives			✔	If a deception solution generates more alerts than you can monitor, it's got a basic design flaw. We've designed our alerting algorithms to ensure IllusionBLACK will alert you only when really need to know. It's so accurate, we even do phone alerts.
Private threat intelligence decoys			✔	Reconnaissance is the first step in the kill chain. Detecting targeted reconnaissance means you can detect an attack before it even starts hitting your systems. IllusionBLACK is the only deception solution that offers this private threat intelligence with our reconnaissance decoys.
Persona decoys			✔	Social engineering is the #1 attack vector in targeted attacks. Deception solutions that can't detect attacks against your people are missing possibly the most crucial stage in the kill chain. IllusionBLACK can create decoy personas to detect social-engineering and spear-phishing attacks.
ThreatParse ™ Natural language attack reconstruction.			✔	Many solutions give you raw attack logs that are hard to understand and waste precious incident response time. IllusionBLACK's ThreatParse ™ reconstructs the entire attack to natural language, so your response team can act rather than analyse. IllusionBLACK can also visually replay an entire attack from start to finish, taking the guess-work out of "what happened" and when.

SMOKESCREEN

Capability	Open-source honeypots	Other deception providers	Smokescreen's IllusionBLACK	Why it matters to you
Active directory deception			✔	Active Directory is the 'phone book' for a modern attacker. Many solutions don't deploy deception here, meaning real attackers will miss their decoys entirely! IllusionBLACK fully integrates deception with your Active Directory to ensure attackers always hit decoys when performing lateral movement.
Decoy uniqueness			✔	Some solutions just run a few virtual machines with multiple IP addresses, meaning you only have 5 or 6 actual decoys. This won't fool even the most basic attacker. IllusionBLACK can make hundreds of individually unique, individually customisable decoys.
Data decoys			✔	Information is what the attacker has actually come for. If a deception solution cannot deploy data decoys, it will miss the final phase in the kill chain. IllusionBLACK can create multiple types of data decoys that can be deployed everywhere from a USB stick to a mobile device.
MirageMaker ™ Automatic dataset and bait generation.			✔	Ok, so you've made 100's of decoys. How do fill them with realistic content? Most solutions either don't customise at all, or let you put some custom files in a few virtual machines. IllusionBLACK has out of the box auto-generation of decoy data, including credit cards, SSNs, files, credentials and much more. Not just does this make your decoys ultra-realistic, it saves you weeks worth of deployment time that others will gloss over.
ThreatDeflect ™ On-the-fly attack redirection.			✔	If you've got an attacker in your network, we can redirect them into a virtual cloud of decoys, so they aren't even sitting in your network anymore. Other systems may only keep an attacker busy for a few minutes, With ThreatDeflect ™, we can keep them busy for days.
Custom-built decoys and integrations			✔	Smokescreen is the only company that offers custom-built decoys and integrations. If your environment has a specific system that we don't cover, we can build it specifically for you.
Security and reliability			✔	Many solutions are just running VM's on a standard Linux distribution. IllusionBLACK runs on Smokescreen's custom, hardened build of BSD UNIX, known for it's legendary security and reliability. We also do not use any public / open-source honeypots under the hood.
Experience			✔	Smokescreen's team has deployed deception for over 10 years in several ultra high-security environments. We've personally run successful deception campaigns, catching apex attackers on multiple occasions. All that front-line experience has gone straight into IllusionBLACK. We're ***the*** deception specialists, so we know how to do it right.

Dont’ take our word for it.
Hear what our customers say.

“Outperforms market leading solutions that cost significantly more”
Executive VP - Multi-National Infrastructure Company

“Detects threats much more effectively than conventional monitoring.”
CTO - Digital Payments Provider

“Uncovers lateral movement and substantially improves internal network visibility.”
CSO - Leading Private Sector Bank

SMOKESCREEN

DETECT | DEFLECT | DEFEAT

www.smokescreen.io | info@smokescreen.io