ACTIVE DEFENSE RESOURCES

Smokescreen Deception MITRE Shield Mapping

SMOKESCREEN

Smokescreen Provides 95% Coverage for MITRE Shield Techniques

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Decoy Account	Application Diversity	Application Diversity	Application Diversity	Burn-In	API Monitoring
Application Diversity	Decoy Account	Decoy Network	Behavioral Analytics	Behavioral Analytics	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Content	Detonate Malware	Decoy Account	Decoy Content	Burn-In	Decoy Content	Decoy Account
Decoy Content	Decoy Credentials	Isolation	Decoy Content	Decoy Credentials	Decoy Account	Decoy Credentials	Decoy Content
Decoy Credentials	Decoy Network	Migrate Attack Vector	Decoy Credentials	Decoy Network	Decoy Content	Decoy Diversity	Decoy Credentials
Decoy Network	Decoy System	Network Manipulation	Decoy Network	Email Manipulation	Decoy Credentials	Decoy Network	Decoy Diversity
Decoy Persona	Detonate Malware		Decoy System		Decoy Diversity	Decoy Persona	Decoy Network
Decoy Process	Email Manipulation		Email Manipulation		Decoy Persona	Decoy Process	

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Decoy System	Network Diversity	Security Controls	Hunting	Isolation	Decoy System	Decoy System	Decoy Persona
Detonate Malware	Network Monitoring	Software Manipulation	Isolation	Network Manipulation	Network Diversity	Network Diversity	Decoy System
Migrate Attack Vector	PCAP Collection		Network Manipulation	Security Controls	Network Manipulation	Pocket Litter	Detonate Malware
Network Diversity	Security Controls		Network Monitoring	Standard Operating Procedure	Pocket Litter		Migrate Attack Vector
Network Manipulation	System Activity Monitoring		PCAP Collection	Software Manipulation	Security Controls		Network Diversity
Pocket Litter	Software Manipulation		Pocket Litter		Software Manipulation		Network Manipulation
Security Controls			Standard Operating Procedure				Pocket Litter
Software Manipulation			System Activity Monitoring				Security Controls
							Software Manipulation

How Smokescreen Covers These Techniques

	Shield technique	How we do it
1	Admin Access	High interaction decoys and endpoint decoys identify the use of administrative credentials and any attempts to bypass protection controls.
2	API Monitoring	Endpoint deception monitors system calls, from code execution to file access, to detect local and remote adversarial activity.
3	Application Diversity	Comes preloaded with decoy applications for a variety of industries and use cases. Defenders can instantly plant these seemingly realistic decoys that blend in with your network making it difficult for attackers to move without encountering one of them. The platform also provides defenders with the ability to create custom decoys with properties of their choosing.
4	Behavioral Analytics	Network and endpoint deception include numerous capabilities to identify unusual behavior along with triage information to expedite analysis and resolution.
5	Burn-In	Endpoint decoys can automate burn-in by deploying application-specific lures like saved sessions, passwords, cookies, bookmarks, and files. The content of each of these is tied to existing network deception and is customized to fit the user's profile. These are automatically updated to align with changes in network deception and can be augmented with additional customization and burn-in.
6	Decoy Account	Can set up, monitor, and seed decoy local, domain and cloud accounts automatically. Lures are placed in both frequently-targeted and infrequently-accessed locations to detect account enumeration and privilege escalation attempts.
7	Decoy Content	The platform’s decoy generation includes a diverse set of content, including applications, files automatically-customized to various roles, ICS device profiles, and additional custom services. Defenders also get the ability to create customized datasets that can be deployed on decoy services.

How Smokescreen Covers These Techniques

	Shield technique	How we do it
8	Decoy Credentials	Defenders can use the platform to add decoy credentials on macOS, Windows, and Linux for various applications and services. Credentials are spread across Microsoft Office files, the registry, and configuration files.
9	Decoy Diversity	The platform comes pre-loaded with decoys that mimic applications and services used in a variety of industries including insurance, banking, healthcare, legal, energy, IT, healthcare, and more. All of these decoys run the appropriate services to automatically fit various environments they may be deployed in. Additionally, defenders get the ability to create custom personalities for decoys that can address specific industry and niche use cases.
10	Decoy Network	Defenders get the ability to set up a deceptive network, integrate decoys into existing networks, and redirect attacks from existing networks into deceptive networks for contained post-compromise engagement.
11	Decoy Persona	The platform can create persona decoys with multiple contact points to enhance realism, and combined with other types of deception to enhance discoverability both internally and on the public Internet, albeit only for adversaries.
12	Decoy Process	The platform has the ability to create decoy processes to detect defense evasion attempts. These can also be used to encourage / discourage attacks against specific targets.
13	Decoy System	Creates systems built using a standard organizational software image or using selections of specific services. These can be used to create decoy systems customized to serve as attack targets for specific attack scenarios. Additionally, lures can be deployed on real user systems to enhance the authenticity of the decoy systems and draw adversaries to engage with them.
14	Detonate Malware	Decoys can be customized to fit a variety of system profiles and serve as tailored environments for malware detonation, analysis, and IOC collection.

How Smokescreen Covers These Techniques

	Shield technique	How we do it
15	Email Manipulation	Defenders can set up mail flow rules to forward suspicious emails to Smokescreen's decoy email inboxes.
16	Hunting	Smokescreen's investigation capability, ThreatParse, helps hunt teams quickly identify activity based on the severity of impact as against simply volume or severity of the action. Defenders benefit from the platform's hunt-focused design and capabilities, and coupled with ThreatParse, significantly speed up hunt missions and information gathering exercises.
17	Isolation	Endpoint deception can suspend processes, impeding attackers' ability to continue execution and expand the engagement, or to connect to C2 infrastructure.
18	Migrate Attack Vector	Malicious content or executables can be moved to a decoy or network for contained post-compromise interaction and analysis. Defenders get access to detailed telemetry on all the activities performed by the malicious code.
19	Network Diversity	Comes preloaded with decoy applications for a variety of industries and use cases. Defenders can instantly plant these seemingly realistic decoys that blend in with your network making it difficult for attackers to move without encountering one of them. The platform also provides defenders with the ability to create custom decoys with properties of their choosing.
20	Network Manipulation	Defenders can add a kill switch or route specific malicious activity to a decoy network to stop adversary connections or change the network rules within a decoy network to interfere with the adversary communications to understand their behavior and TTPs.
21	Network Monitoring	Defenders get the ability to monitor traffic sent to decoys to detect network reconnaissance attempts and can also detect MiTM attempts used to capture credentials for subsequent use during an attack.

How Smokescreen Covers These Techniques

	Shield technique	How we do it
22	PCAP Collection	The platform captures all network traffic sent to and from network decoys and presents an analysis.
23	Pocket Litter	The platform has the ability to create realistic and customizable pocket litter based on the network or endpoint personality. These can be placed on decoy file shares, FTP servers, and real user endpoints to reinforce the legitimacy of a system or user.
24	Security Controls	Endpoint and network deception make systems appear vulnerable for adversary engagement without actually being vulnerable to the attacks. High-interaction decoy services can be set up with varying levels of restrictions to facilitate or restrict adversary activity to gather information on TTPs and tools.
25	Standard Operating Procedure	Active Directory decoys and high interaction decoys monitor activity like user creation, deletion, and modification to detect any activity occurring beyond the defined SOP.
26	System Activity Monitoring	High interaction decoys and endpoint deception monitor system activity to detect threats and malware.
27	Software Manipulation	The platform gives defenders the ability to feed adversary interactions with false data pointing to a decoy network.

About Smokescreen

Smokescreen is a pioneer in deception-based active defense solutions. It is the company of choice for offensive security teams, with a customer Net Promoter Score of 70.

Our deception platform protects many of the world's most targeted organizations including leading financial institutions, energy companies, manufacturing giants, and technology majors.

The company comes from a red team and offensive security heritage. It finds a mention in every deception report published by Gartner and has been featured in Fortune Magazine and Bloomberg.

Email: info@smokescreen.io
Web: www.smokescreen.io