ILLUSIVE PLATFORM FEATURE BRIEF:

Network Device Emulations

Routers, switches, printers and other network devices are increasingly under fire from DDoS and other disruptive attacks. These devices are always on, seldom updated and often configured to default settings, and attackers use them to perform reconnaissance undetected as they plan their next hop towards exfiltrating sensitive data. The wide range of available network devices, and the difficulty of supporting and updating all of them, has created a gap that legacy security stacks struggle to effectively fill. Illusive crafts a web of highly authentic emulations of typical network devices designed to trick attackers into interacting with them, allowing your organization to detect and stop threats against network communications infrastructure without complex deployments or business interruptions.

BENEFITS

- High-fidelity and frictionless network infrastructure attack detection
- Blanket your network with thousands of deceptive switches, routers, printers and much more with a click
- Customized emulations of any network devices your organization uses
- Fill network device security gaps seamlessly and rapidly with no business or connectivity disruptions

Identify Network Device Attacks

Collect Forensics and Intelligence

Plant deceptive network device emulations, as well as endpoint data deceptions that point towards them as lures, to fool attackers into engagement. As soon as attackers interact with the emulations, they notify organizations about their presence.

Capture data about attacker tactics and methods, including the commands entered through the command line interface, screenshots with attack evidence, and more.

How Network Device Deceptions Work

1. Choose the network device emulations your organization would like to deploy from the Illusive catalog of preconfigured and tailor-made options
2. Distribute emulations of network devices and breadcrumbs leading to them throughout your servers, systems and endpoints
3. Attackers seeking to hack your organization's network devices can't tell real machines from fake; disoriented, they click on the emulations
4. Upon clicking the deceptive network device, an incident report is sent to the organization with forensics on the attacker and their methods