**01 - AL Jammaz’s LinkedIn Page:**

(The message)

Reveal #Attackers with Deception #Technology. With #Singularity #Hologram uncover covert attackers. Singularity Hologram’s deception technology not only serves to detect and respond to active attackers in your environment, but also to inform and strengthen your #security program in the longer term.

**02 - AL Jammaz’s Twitter Page:**

Reveal #Attackers with Deception #Technology. With #Singularity #Hologram, uncover covert attackers with high-interaction decoys that mimic production assets.

**03 - Landing page – Al Jammaz website:**

(The message)

**Singularity Hologram**

**Who’s looking and what are they after?**

Adversaries with an established foothold in the environment will at some point attempt lateral movement. Similarly, employees with privileged access and a motive for misuse may pose an insider threat.

Singularity Hologram, a component of the SentinelOne Singularity XDR platform, leverages advanced, high-interaction deception and decoy technology to lure in-network attackers and insider threat actors into engaging and revealing themselves. By mimicking production OSes, applications, data, and more, Singularity Hologram uncovers covert adversary activity, collects high-fidelity telemetry, and garners actionable intelligence to help you build your defenses.

**Cast a Wide Net**

Entice adversaries performing reconnaissance with mimicked production OSes, applications, data, ICSes, IoT, cloud functions, and more.

**Identify Active Compromise**

Snare adversaries and insiders lurking across your network as they move laterally and interact with lures and decoy assets.

**Visualize & Strengthen**

Quickly visualize attacks on the network, watch how they play out over time, and apply these learnings to strengthen your defenses.

**Expand & Collect**

Integrate with Singularity IdentityTM threat detection and response (ITDR) for holistic endpoint and Active Directory protections.

**Trap Even the Most Covert Adversaries**

Singularity Hologram network decoys detect and alert you of imminent threats and activities in your environment that prevalently target enterprises today:

• Man-in-the-Middle (MitM) activity

• Ransomware and other malware

• Advanced persistent threats (APTs)

• Reconnaissance activity

• Insider threats

Singularity Hologram decoys appear indistinguishable from production assets, and are designed to engage and misdirect attackers away from real systems and data. All decoys encompass a breadth of form factors, adapting to a variety of business & organizational needs. These include:

• Decoy ICS-SCADA industrial control systems

• Decoy emulations for SWIFT terminals, point-of-sale (POS) systems, VoIP telecom

systems, network routers & switches, and IoT specialty devices

• Decoy Windows and Linux OSes

• Decoy Serverless and storage cloud technologies

**Maximize Your Insight Into the Adversary**

Singularity Hologram’s deception technology not only serves to detect and respond to active attackers in your environment, but also to inform and strengthen your security program in the longer term.

By misdirecting attacks using Singularity Hologram, you gain ingestible, actionable TTP infor- mation and high-confidence, substantiated attack forensics that can support investigations. Hologram even lets you visualize attacks, see how they progressed over time, and map their associated events to the MITRE ATT&CK D3FENDTM matrix. From Hologram, you can reduce your future mean time to respond with automated, repeatable processes and playbooks.

**04 – Attach the datasheet**