USE CASE

Use Deception Technology to Protect Vulnerable Legacy Systems

Shielding critical–but vulnerable–systems against modern day threats

The constant evolution of technology leaves businesses with the widespread challenge of legacy systems. With each new software release, organizations can choose to upgrade or replace existing operating systems and their components or keep legacy systems running out-of-date and possibly vulnerable software, introducing risks. Due to the vast technology footprint of enterprises, legacy systems are present across IT, OT, IoT, and specialized infrastructure. These legacy systems represent attractive targets for threat actors who use unpatched vulnerabilities as an easy entry and pivot point into an enterprise.

THE POWER OF DECEPTION IN THREAT DETECTION

Commvault recognized organizations' need and challenge to keep legacy systems in use within their environments. To help protect them and build the cyber resilience of organizations, we integrated an early warning mechanism to our platform that spots exploitation attempts of legacy systems across production instances using decoys, allowing for attackers to be found and removed before they reach critical applications and data. By inserting look-alike and vulnerable—but decoy—systems alongside real assets, we bait attackers into attacking threat sensors that mimic the old legacy assets. This triggers high fidelity alerts upon first touch and creates an early detection layer that safeguards your vulnerable legacy systems to mitigate their risk without causing interruptions in the systems.

Microsoft usage reports highlight that older, out-of-support, legacy operating systems account for more than 10% of all production systems.[1]

Deception technology like this has recently had endorsements in the industry, for example, Kevin Mandia's keynote speech at RSA 2023[2] advocates the use of cyber deception. Also, a recent report in the Telegraph Newspaper[3] and an academic paper[4] on the validity of deception technologies as an additional tool in the battle against cyber-attacks.

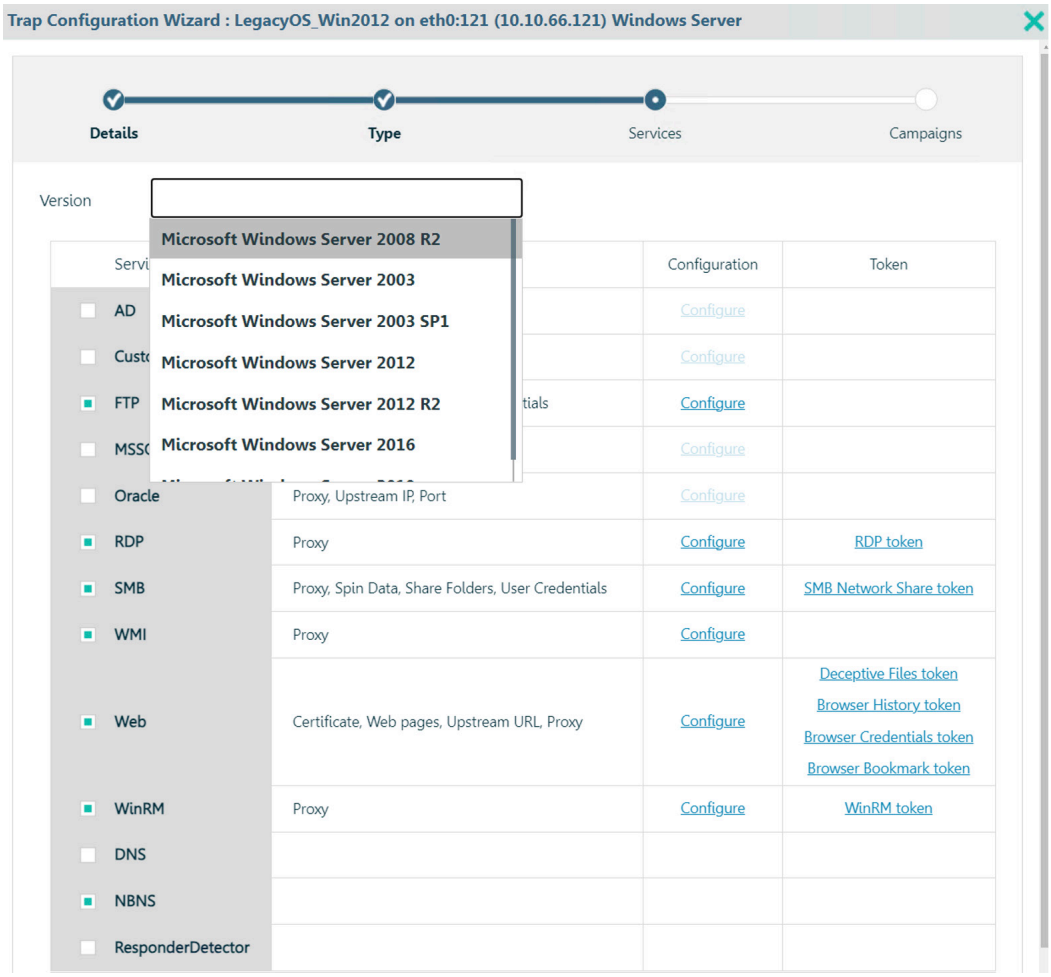
APPLIED EARLY WARNING: SHIELDING LEGACY WINDOWS SERVERS

Commvault's deception-based early warning provides various possibilities to protect legacy systems across on-premises, cloud, and hybrid environments. For this paper we will focus on the example of threat actors targeting Windows Server 2012 that leverage known vulnerabilities associated with this specific operating system version.

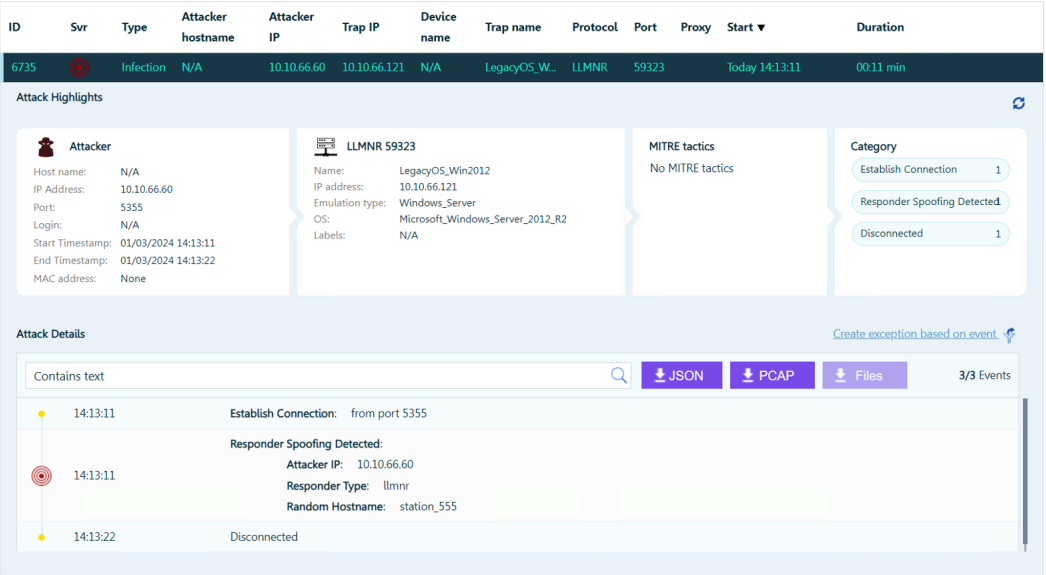
General considerations for **vulnerabilities** in **Windows Server 2012**

1. **Unpatched Security Flaws:** Exploiting vulnerabilities that haven't been addressed through updates and patches.
2. **Weak Authentication Protocols:** Attackers may target deprecated or weak authentication methods to gain unauthorized access.
3. **Remote Desktop Services Exploits:** Vulnerabilities in services like Remote Desktop Protocol (RDP) could be targeted for unauthorized access.
4. **Web Server Vulnerabilities:** If Windows Server 2012 is hosting web services, attackers might exploit vulnerabilities in web server software.

In this example, 100 real Windows Server 2012 assets that cannot be upgraded and are critical for core business processes are protected with 200 lightweight Threatwise sensors based on our preconfigured Windows Server template, easily managed through the configuration wizard. Real Microsoft services are emulated by the threat sensors on IP addresses that detect recon of attackers on your network without requiring additional Microsoft licensing.



To align cyber risk to the businesses risk tolerance, one unpatched live server in the subnet is surrounded by two decoy servers. While staying invisible to company employees and vulnerability scanners, Threatwise sensors trigger high-fidelity alerts in real time based on bad actors' activity such as scans, connects, or manipulation. Malicious activity is recorded and enriched with advanced threat intelligence data, sent to key IT and security stakeholders, and integrated into SIEM or SOAR workflows and playbooks.



While we focused on Windows Server 2012 in this example, you can create numerous Microsoft Windows legacy operating systems using preconfigured sensor templates, such as Windows Server 2003, Windows 7, or Windows XP. Additionally, create personalized templates in seconds with the adaptive sensor that fingerprints your existing legacy systems, generating flawless look-alikes.

1 https://www.spiceworks.com/it-security/endpoint-security/guest-article/bridging-the-legacy-security-gap/
2 https://www.youtube.com/watch?v=awUglvaa1dQ
3 https://www.telegraph.co.uk/business/2023/08/29/national-grid-honeypots-catch-hackers-cyber-attacks-infra/
4 https://www.researchgate.net/publication/348198038_Design_Thinking_for_Cyber_Deception

See Threatwise in action and request a demo or free trial at **commvault.com/platform/threatwise**