THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | September 14th, 2024

CSCI 6015: Homework-4
CrowdStrike 2024 Report: Trends in Cybercrime for Singletree

The CrowdStrike 2024 Global Threat Report highlights two critical trends in cybercrime that pose significant threats to Singletree Engineering. The rapid evolution of cloud-based threats and identity-based social engineering attacks presents new challenges for organizations relying on digital infrastructure and cloud environments. This report outlines these two trends in detail and provides a comprehensive action plan to mitigate their impact on Singletree Engineering.

1. Cloud-Conscious Attacks

According to the CrowdStrike 2024 report, cloud intrusions have increased by 75% year-over-year (YoY), with 84% of these attacks attributed to eCrime actors (CrowdStrike, 2024). The shift towards cloud-conscious adversaries, who are increasingly aware of how to exploit vulnerabilities in cloud-based infrastructure, is a growing concern. These attackers target cloud workloads and abuse features unique to the cloud, such as data exfiltration from storage services like SharePoint or GitHub.

Singletree Engineering, if reliant on cloud infrastructure for critical operations, faces an elevated risk of data breaches, identity theft, and lateral movement within cloud environments. The organization's exposure to such threats is amplified if cloud services are not adequately secured or monitored.

2. Identity-Based and Social Engineering Attacks

The CrowdStrike 2024 report also highlights a surge in identity-based attacks, with adversaries focusing on credential theft (CrowdStrike, 2024). These attacks often bypass traditional security measures like multi-factor authentication (MFA) through sophisticated techniques such as SIM-swapping, phishing, and the use of stolen API keys and session tokens. Given Singletree Engineering's likely dependence on secure identity management, these types of attacks could lead to significant breaches if security protocols are compromised.

Action Plan to Mitigate Threats

1. Enhance Cloud Security

To counter the increasing threat of cloud-conscious attacks, Singletree Engineering should prioritize cloud security by implementing continuous monitoring tools, such as the CrowdStrike Falcon® platform. These tools can detect unauthorized access attempts and unusual data movement in real-time. Additionally, multi-layered protection should be integrated within cloud environments to address vulnerabilities in both infrastructure and applications. Regular security audits and penetration testing will ensure that misconfigurations are detected and remediated promptly.

2. Strengthen Identity Management and Protection

Singletree Engineering should adopt a Zero Trust framework (ZTF) where no implicit trust is granted to any user, even within the network. This framework enforces strict verification for every user and device attempting to access sensitive data. While MFA is still crucial, using more advanced methods such as biometric verification or hardware-based security keys will further reduce the risk of identity-based attacks. In addition, security awareness training for employees will help them recognize phishing and social engineering attempts, which are commonly used by adversaries to steal credentials.

References

CrowdStrike. (2024). CrowdStrike 2024 Global Threat Report. CrowdStrike. https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

***** END OF DOCUMENT *****