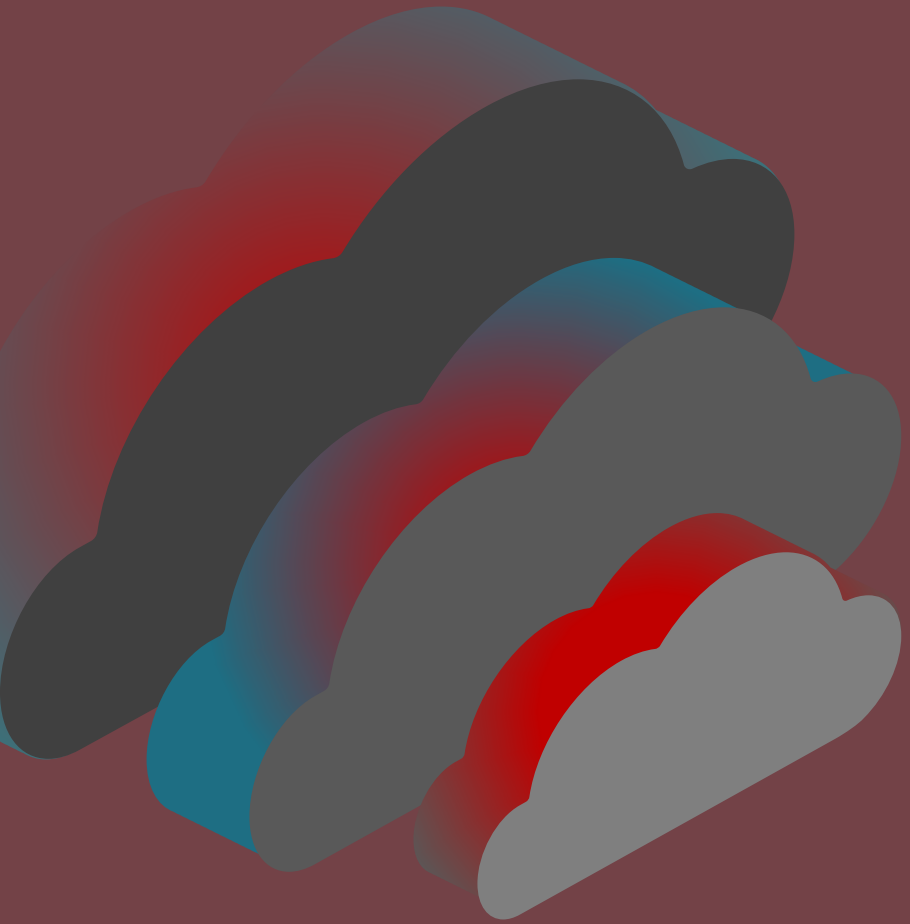

# Recon: BLACK

secureCENTRX

Proof of Value

Vulnerability Managed Services

Unifying All Dimensions

# Advanced Persistent Threaths

- APT groups are targeting IT, telecoms, utilities, industry control systems, aviation, automotive, academic, pharmaceutical, government and security sectors around the world.
- These threats continue to rise over the years as these threat groups continually improve their tradecraft.
- SolarWinds attack proved that APTs can leverage supply chain attacks and use the existing managed services in a compromised organization's environment.
- REvil Ransomware-as-a-Service (RaaS) organization, most recently attacked meat supplier JBS, which ultimately paid $11 million to get its processing plants back online.
- Kaseya Ransomware infected more than 1,500 organizations.

# Recon: Black – Initial Reconnaissance

***secureCENTRX employs advanced collection of target customer's information to attempt to identify any and all security misconfigurations and vulnerabilities within the customer's external environment. This method seeks to identify a path real-world attackers would use in a targeted attack against the customer.***

**Methods of Reconnaissance:**

- **Utilizing search engines:** Using Google, Bing, and other search engines to extract information such as username, password, hidden web pages, technology, file metadata, company information etc., that can be used to target systems, data, and employees of the company.
- **Certificate Transparency:** Identify issues related to SSL/TLS encryption from customer's external applications and installed certificates.
- **Enumeration:** secureCENTRX employs multiple automated and manual scanning techniques to identify the organization's entire external footprint. This information is then used to conduct further unobtrusive checks including asset identification, port scanning, and vulnerability scanning. secureCentrx employs subdirectory identification on any and all external facing web applications.
- **Standard:** secureCENTRX classifies findings using OWASP and MITRE ATT&CK frameworks to provide detailed results by leading industry standards.

***This information is then collected, any and all vulnerabilities and misconfigurations are organized into a customized report for the customer. Remediation recommendations are provided within the report and the debrief with the customer. A "Proof-of-Value" for each finding is provided whereby, secureCENTRX reports of the impact and risk rating of the finding.***

# Optional - Vulnerability Scanning and Internal Penetration Testing

If permitted and with collaboration, we would like to provide the optional Recon: Black vulnerability assessment services

- **Vulnerability Scanning:** Nessus Vulnerability Scanning
  Asset Discovery
- **Internal Penetration Testing:** Horizon3.ai NodeZero Internal Autonomous Penetration Testing.
- **Review:** Findings Readout and initial Vulnerability Review

# Proof of Value - “Try and Keep” – For 1 Year

CROWDSTRIKE

## Managed Security Reimagined

Our commitment to providing Cyber Security to the free market is always Top Of Mind.  Our partnerships with leading security manufactures allows us meet our commitment by providing non-trivial impact to those who entrust us with their most critical assets.  This is our way of saying “thank you” to our new relationships.

- 50 Licenses – CrowdStrike Falcon Advance Defend (Complete + Defend + Insights + Discover + Threat Graph)
- 24/365 Crowdstrike Overwatch – SOC Services with Active Threat
- 24/365 secureCENTRX Security Operations Center – Follow the Sun Monitoring, Alerting, Reporting and Advisory
- 12-Month Complimentary – NO OBLIGATION – NO AUTOMATIC RENEWALS

# secureEVERYTHING

Unifying All Dimensions

secureCENTRX.com | an M-Theory Company