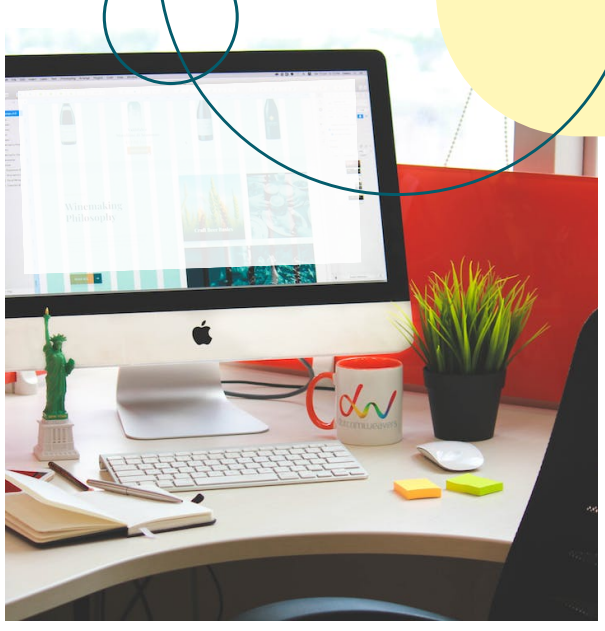
Indicators of Compromise (IoCs)



Common Indicators of Compromise (IoCs) used by cybersecurity teams include:

01 Malicious IP Addresses:

Identifying IP addresses associated with known malicious activities or command and control servers.

02 Malware Signatures:

Recognizing specific patterns or signatures of known malware through signature-based detection.

03 Unusual Network Traffic Patterns:

Monitoring for abnormal patterns in network traffic that may indicate a potential compromise.

04 Suspicious Domains:

Identifying domains that are newly registered, closely resembling legitimate domains, or known for malicious activities.

05 Anomalous User Behavior:

Detecting unusual user activity, such as multiple failed login attempts or access from unfamiliar locations.

06 Command and Control Servers:

Tracking communication with servers that are commonly associated with controlling malware or malicious activities.

07 Unexpected Outbound Traffic:

Monitoring for unexpected data exfiltration or communication leaving the network.

08 File Hashes:

Identifying unique file hashes associated with known malware or compromised files.

09 Phishing Indicators:

Recognizing indicators related to phishing, such as suspicious email addresses or deceptive URLs.

10 Registry Changes:

Monitoring changes to the Windows registry, as malicious software often modifies registry entries.

11 Unusual System Processes:

Detecting processes or services running on systems that are not typical for normal operations.

12 Abnormal System Resource Usage:

Identifying unusually high CPU, memory, or disk usage that may indicate a compromise.

13 Unexpected Software Modifications:

Detecting unauthorized changes or modifications to critical system files or software.

14 Credential Anomalies:

Monitoring for unauthorized access or usage of credentials, including credential stuffing or brute force attacks.

15 Geographical Anomalies:

Recognizing login attempts or access from unusual geographical locations compared to normal user behavior.

16 Malicious URLs:

Identifying URLs known for hosting malicious content or used in phishing campaigns.

17 Registry Key Changes:

Monitoring for changes to critical registry keys that may indicate malicious activities.

18 Email Header Anomalies:

Analyzing email headers for irregularities that may suggest a phishing attempt or email compromise.

19 Newly Created User Accounts:

Recognizing the creation of new user accounts that are not part of regular onboarding processes.

20 Exploit Attempts:

Identifying patterns or signatures associated with attempted exploitation of vulnerabilities.

www.centextech.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road, Suite #1100
Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree ST NE,
400 Colony Square #200
Atlanta, GA 30361

Phone: (404) 994 - 5074

Capital Factory, 701 BrazosStreet,
Suite 500 Austin, TX 78701

Phone: (512) 956 - 5454