CIRT Playbook Battle Card: **GSPBC-1025 - Credential Access - Unsecured Credentials**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Limit credential overlap across accounts and systems
5. Ensure that servers and workstations are logging to a central location
6. Implement password policies that:
   a. Require strong passphrases
   b. Prohibit password storage in the registry and within insecure files
   c. Recommend storing passwords on separate cryptographic hardware
7. Conduct employee security awareness training

(I) Identification

1. Watch processes and command-line arguments for indicators of credential searching
2. Monitor for:
   a. Unusual permission modification
   b. Abnormal file access
   c. Unexpected account creation
   d. Atypical reading of .bash_history
3. Investigate and clear ALL alerts associated with impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Remove the affected system from the network
5. Lock any accounts that exhibit suspicious behavior
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Review logs to determine which accounts were accessed
5. Inspect all affected accounts
6. Search file systems and logs to determine if insecure credentials were collected
7. Reset the passwords of any compromised accounts
8. Patch asset vulnerabilities
9. Remove all instances of credentials that were stored insecurely

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk

References:

1. MITRE ATT&CK Technique T1552: https://attack.mitre.org/techniques/T1552/

Resources:

- ➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT