John McGloughlin

john.mcgloughlin@guardsight.com

https://www.linkedin.com/in/mcgloughlin

Playbook Battle Cards

PICERL Cheat Sheets

Background

PLAYBOOK BATTLE CARDS

➤ **Recipes for preparing and applying countermeasures against cyber threats and attacks**

➤ **Prescriptive approach to combat various TTP deployed by cyber threat actors**

➤ **Follow a PICERL model**

➤ **Aid the kinetic activities conducted by humans prior to, during, and after cybersecurity incident response**

➤ **Inspired by CERT Societe Generale**

CIRT Playbook Battle Card: **GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware**

(P) Preparation	(I) Identification	(C) Containment

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Examine file shares for loose/open privileges
4. Maintain Antivirus/EDR application updates
5. Create network segmentation
6. Log traffic between network segments
7. Incorporate threat intelligence
8. Incorporate deception technology
9. Perform routine inspections of asset backups
10. Validate proper functionality
11. Confirm backups are free of malware
12. Establish ability to pay ransoms w/cryptocurrency
13. Obtain decryption keys for ransomware variants
14. Confirm cybersecurity insurance coverages
15. Conduct ransomware simulations
16. Conduct phishing simulations
17. Conduct user awareness training
18. Conduct response training (this PBC)
	1. Monitor for:
	  a. Ransomware notes/messages
	  b. Unusual file extensions or malicious extensions
	  c. User reports of files being corrupt or not readable
	  d. Emails with suspicious attachments
	  e. Unusual DNS traffic
	  f. High velocity renaming of files
	  g. CPU spikes on file sharing systems
	  h. Unusual userland executable binaries
	  i. Anomalous network connections on hosts
	  j. Firewall denies to well known file sharing ports
	  k. Network connections to known C2 and exploit kit locations
	  l. Use of TOR or I2P
	2. Investigate and clear ALL alerts of possible ransomware
	  a. IDS/IPS
	  b. Antivirus/EDR
	  c. Threat intelligence
	  d. Deception technology
		1. Inventory (enumerate & assess)
		2. Detect
			Deny	Disrupt	Degrade	Deceive	Destroy
							3. Observe -> Orient -> Decide -> Act
							4. Locate and isolate the assets responsible for encrypting files
							5. Isolate impacted file sharing systems
							6. Close the attack vector
							7. Fortify non-impacted file sharing systems
							8. Fortify non-impacted critical assets
							9. Issue perimeter enforcement for known threat actor locations
							10. Deploy EDR hunter/killer agents and terminate offending processes

(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
1. Close the attack vector 2. Patch asset vulnerabilities 3. Re-image impacted assets 4. Inspect all assets for IOC consistent with the attack profile 5. Inspect user activity for IOC consistent with the attack profile 6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery 7. Implement newly obtained threat signatures	1. Restore to the RPO within the RTO 2. Restore from known clean backups 3. Address collateral damage	1. Perform routine cyber hygiene due diligence 2. Engage external cybersecurity-as-a-service providers and response professionals 3. Avoid opening email and attachments from unfamiliar senders 4. Avoid opening email attachments from senders that do not normally include attachments Notes: 1. Report cybercrime: https://www.ic3.gov/default.aspx 2. Paying ransoms is discouraged but should be a contingency available to executives (SEE Preparation #12)

GUARDSIGHT
© GuardSight, Inc.® | https://www.guardsight.com

GUARDSIGHT

Implementation

DERIVED FROM GOOGLE DOCS
TEMPLATE (GS-CIRT-PBC-Template) ➡️
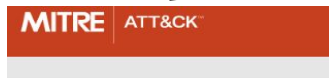
GS-CIRT-PBC-Template   In template gallery ⭐ 📁
File Edit View Insert Format Tools Add-ons Help

REFERENCE MITRE ATT&CK TTP

FOLLOW A PICERL MODEL

MITRE | ATT&CK

ENTERPRISE ▾

TACTICS

All

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

MITRE | ATT&CK

ENTERPRISE ▾

TECHNIQUES

All

Initial Access   -

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Replication Through Removable Media

Spearphishing Attachment

Spearphishing Link

Spearphishing via Service

Supply Chain Compromise

Trusted Relationship

Valid Accounts

SANS 504-B Incident Response Cycle: Cheat-Sheet   v1.0, 11.5.2016 – kf / USCW

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)

Preparation
- People   - Policies   -Tools   - Training
- Notes   - Procedures   - Mgt Tng   - Jump Bag
- Relationships   - Coms plan

Identification
- Awareness   - Alert Early   - Primary IR Handler   - Unusual Files
- Need to Know   - Use OOB Comms   - Passive monitoring   - Analyze Logs
- Unusual processes - New Accts / Privs - Odd Sch Tasks   - Chain of Custody
- Unusual Security Evts

Containment
- Stop Bleeding   - Short-term   - Back-up   - Long-term
- Categorize   - Criticality   - Sensitivity   - Document Actions
- Notify Mgt   - Asgn Primary IRH - Low Profile   - Infected Vlan
- Remove LAN Cbl   - FW/IDS Filters   - ISP coord   - Forensic Images
- Memory Captures - Adjacent Host Logs - Patch Exploited Vuln(s)
- Chg Pswds   - Kill Backdoors

Eradication
- Del Artifacts   - Root Cause   - Restore Back-up   - Remove Malware
- Apply All Patches - Addl FW / IDS Filters - Chg DNS Names   - Rescan network
- Black Hole IP's - Seek other Host footholds - Wipe/Format/Rebuild

Recovery
- Return to Ops   - Test /Doc Baseline   - Move to Production (Approval)
- Monitor (signs/shells/artifacts/events)   - Script searches for attacker artifacts

Lessons Learned
- Document Incident   - Immediately upon recovery Phase   - Assign to on-Scene IRH
- All affected parties review / comment on draft   - Reach Report Consensus
- Finalize Report   - Provide Exec Summary   - Address Process not people
- Seek Required Changes   - Seek Funding   - Update Procedures

GUARDSIGHT

Value Creation

➜ **PROVIDES RESPONSE TEAMS WITH LIGHTWEIGHT CHEAT SHEETS**

➜ **DISPENSES SYSTEMATIC PROCESS FOR CYBER BATTLE RESPONSE**

➜ **TURNS THE "*PUCKER MOMENT*" INTO "*CONFIDENT RESPONSE*"**

➜ **CONVERTS CHAOS INTO ORDER**

➜ **ORGANIZES FORCE CONCENTRATION**

➜ **PRESENTS A QRF TEAM WITH EFFECTIVE CONTAINMENT STRATEGIES**

➜ **SUPPLIES PLANNING FOR PREPARATION & MOVEMENT**

GUARDSIGHT

Operational Excellence

WORK INSTRUCTION (W-1060)

AVAILABLE TO THE PUBLIC
https://github.com/guardsight/gsvsoc_cirt-playbook-battle-cards

W-1060 - How-To Maintain CIRT Playbook Battle Cards

SYNOPSIS

Computer Incident Response Team Playbook Battle Card D

SCOPE

This instruction is intended for team members responsible f

DESCRIPTION

Prologue

Overview

1. Playbook Battle Cards (PBC) are recipes for prepari
2. PBC are a prescriptive approach to combat various
3. PBC follow a PICERL 🗗 model
4. PBC aid the kinetic activities conducted by humans
5. PBC are inspired by https://github.com/certsocietego

ABNF 🗗 **Description Of PBC Title Naming**

'GSPBC' HYPHEN SEQUENCE SHS TACTIC SHS TECHNIQUE DESCRIPTOR ; GSPBC-1000 - Imp
SHS = SPACE HYPHEN SPACE
HYPHEN = '-' ; hyphen
SPACE = ' ' ; whitespace
SEQUENCE = [0-9]{4} ; 1000; starting @ 1000;
TACTIC = INITCAP(ALPHA|SP)* ; Impact; SEE https://attack.mitre.org/tactics/enterprise/ 🗗 (use when
TECHNIQUE = INITCAP(ALPHA|SP)* ; Data Encrypted For Impact; Generic; SEE https://attack.mitre.c
DESCRIPTOR = SHS INITCAP(ALPHA|SP)* ; Ransomware; OPTIONAL industry/layman term

1 NAME
2 SYNOPSIS
3 SCOPE
4 DESCRIPTION
  4.1 Prologue
    4.1.1 Overview
    4.1.2 ABNF Description Of PBC Title Naming
  4.2 Prerequisites
  4.3 Instruction
    4.3.1 Create Using Google Docs
    4.3.2 Publish To GitHub
    4.3.3 Create A GitHub Pull Request
5 EXAMPLES
6 NOTES / BUGS
7 AUTHOR(S)
8 REVIEWER(S)
9 SEE ALSO

guardsight / **gsvsoc_cirt-playbook-battle-cards**

👁 Unwatch ▾ 2   ★ Star 0   ⑂ Fork 0

<> Code   ⓘ Issues 0   Pull requests 0   Projects 0   Security   Insights   Settings

Cyber Incident Response Team Playbook Battle Cards   https://www.guardsight.com   Edit

Manage topics

🕛 **12** commits   ⑂ **2** branches   ◇ **0** releases   👥 **1** contributor   ⚖ MIT

Branch: master ▾   New pull request   Create new file   Upload files   Find file   Clone or download ▾

pivelpin Brewing updates   Latest commit 70125c1 5 hours ago

📁 images	Brewing updates	5 hours ago
📄 GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf	Brewing updates	5 hours ago
📄 LICENSE	Initial commit	14 hours ago
📄 README.md	Brewing updates	5 hours ago

📖 **README.md** ✎

A collection of Cyber Incident Response Playbook Battle Cards

(P) Preparation	(I) Identification	(C) Containment

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Examine file shares for loose/open privileges
4. Maintain Antivirus/EDR application updates
5. Create network segmentation
6. Log traffic between network segments
7. Incorporate threat intelligence
8. Incorporate deception technology
9. Perform routine inspections of asset backups
10. Validate proper functionality
11. Confirm backups are free of malware
12. Establish ability to pay ransoms w/cryptocurrency
13. Obtain decryption keys for ransomware variants
14. Confirm cybersecurity insurance coverages
15. Conduct ransomware simulations
16. Conduct phishing simulations
17. Conduct user awareness training
18. Conduct response training (this PBC)
	1. Monitor for:
	  a. Ransomware notes/messages
	  b. Unusual file extensions or malicious extensions
	  c. User reports of files being corrupt or not readable
	  d. Emails with suspicious attachments
	  e. Unusual DNS traffic
	  f. High velocity renaming of files
	  g. CPU spikes on file sharing systems
	  h. Unusual userland executable binaries
	  i. Anomalous network connections on hosts
	  j. Firewall denies to well known file sharing ports
	  k. Network connections to known C2 and exploit kit locations
	  l. Use of TOR or I2P
	2. Investigate and clear ALL alerts of possible ransomware
	  a. IDS/IPS
	  b. Antivirus/EDR
	  c. Threat intelligence
	  d. Deception technology
		1. Inventory (enumerate & assess)
		2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
		3. Observe -> Orient -> Decide -> Act
		4. Locate and isolate the assets responsible for encrypting files
		5. Isolate impacted file sharing systems
		6. Close the attack vector
		7. Fortify non-impacted file sharing systems
		8. Fortify non-impacted critical assets
		9. Issue perimeter enforcement for known threat actor locations
		10. Deploy EDR hunter/killer agents and terminate offending processes

(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
1. Close the attack vector 2. Patch asset vulnerabilities 3. Re-image impacted assets 4. Inspect all assets for IOC consistent with the attack profile 5. Inspect user activity for IOC consistent with the attack profile 6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery 7. Implement newly obtained threat signatures	1. Restore to the RPO within the RTO 2. Restore from known clean backups 3. Address collateral damage	1. Perform routine cyber hygiene due diligence 2. Engage external cybersecurity-as-a-service providers and response professionals 3. Avoid opening email and attachments from unfamiliar senders 4. Avoid opening email attachments from senders that do not normally include attachments **Notes:** 1. Report cybercrime: https://www.ic3.gov/default.aspx 2. Paying ransoms is discouraged but should be a contingency available to executives (SEE Preparation #12)