



John McGloughlin

john.mcgloughlin@guardsight.com

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

Playbook Battle Cards

PICERL Cheat Sheets

<https://www.guardsight.com> | info@guardsight.com // MIT LICENSE // TLP: WHITE

This document is designated as Traffic Light Protocol (TLP): WHITE.

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

GuardSight® is a registered trademark of GuardSight, Inc.

All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners.

© GuardSight, Inc.

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
<ol style="list-style-type: none"> 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) 	<ol style="list-style-type: none"> 1. Monitor for: <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. IDS/IPS b. Antivirus/EDR c. Threat intelligence d. Deception technology 	<ol style="list-style-type: none"> 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
<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 1. Restore to the RPO within the RTO 2. Restore from known clean backups 3. Address collateral damage 	<ol style="list-style-type: none"> 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 <div> <p>Notes:</p> <ol style="list-style-type: none"> 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) </div>

Implementation

DERIVED FROM GOOGLE DOCS
TEMPLATE (GS-CIRT-PBC-Template)



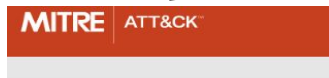
GS-CIRT-PBC-Template

In template gallery



File Edit View Insert Format Tools Add-ons Help

REFERENCE MITRE ATT&CK TTP



ENTERPRISE ▾

TACTICS

All

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact



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

FOLLOW A PICERL MODEL

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

Identification

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

Containment

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

Eradication

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

Recovery

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

Lessons Learned

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

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

Operational Excellence

WORK INSTRUCTION (W-1060)



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

SYNOPSIS	1 NAME
Computer Incident Response Team Playbook Battle Card	2 SYNOPSIS
SCOPE	3 SCOPE
This instruction is intended for team members responsible for	4 DESCRIPTION
DESCRIPTION	4.1 Prologue
Prologue	4.1.1 Overview
Overview	4.1.2 ABNF Description Of PBC Title Naming
1. Playbook Battle Cards (PBC) are recipes for preparing	4.2 Prerequisites
2. PBC are a prescriptive approach to combat various	4.3 Instruction
3. PBC follow a PICERL model	4.3.1 Create Using Google Docs
4. PBC aid the kinetic activities conducted by humans	4.3.2 Publish To GitHub
5. PBC are inspired by https://github.com/certsocieteg	4.3.3 Create A GitHub Pull Request
ABNF Description Of PBC Title Naming	5 EXAMPLES
'GSPBC' HYPHEN SEQUENCE SHS TACTIC SHS TECHNIQUE DESCRIPTOR ; GSPBC-1000 - Imp	6 NOTES / BUGS
SHS = SPACE HYPHEN SPACE	7 AUTHOR(S)
HYPHEN = '-'; hyphen	8 REVIEWER(S)
SPACE = ' '; whitespace	9 SEE ALSO
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.org/techniques/	
DESCRIPTOR = SHS INITCAP(ALPHA SP)* ; Ransomware; OPTIONAL industry/layman term	

AVAILABLE TO THE PUBLIC

https://github.com/guardsight/gsvsoc_cirt-playbook-battle-cards



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

<https://www.guardsight.com> | info@guardsight.com // CONFIDENTIAL // TLP: WHITE

GUARDSIGHT 

(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none"> 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) 	<ol style="list-style-type: none"> 1. Monitor for: <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. IDS/IPS b. Antivirus/EDR c. Threat intelligence d. Deception technology 	<ol style="list-style-type: none"> 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
<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 1. Restore to the RPO within the RTO 2. Restore from known clean backups 3. Address collateral damage 	<ol style="list-style-type: none"> 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 <div data-bbox="1280 816 1875 958"> <p>Notes:</p> <ol style="list-style-type: none"> 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) </div>