



# Playbook Battle Cards

## PICERL Cheat Sheets

<https://www.avertere.com> | [services@avertere.com](mailto:services@avertere.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.

Avertere® is registered trademark of Avertere, LLC.

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

# 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"><li>1. Patch asset vulnerabilities</li><li>2. Perform routine inspections of controls/weapons</li><li>3. Examine file shares for loose/open privileges</li><li>4. Maintain Antivirus/EDR application updates</li><li>5. Create network segmentation</li><li>6. Log traffic between network segments</li><li>7. Incorporate threat intelligence</li><li>8. Incorporate deception technology</li><li>9. Perform routine inspections of asset backups</li><li>10. Validate proper functionality</li><li>11. Confirm backups are free of malware</li><li>12. Establish ability to pay ransoms w/cryptocurrency</li><li>13. Obtain decryption keys for ransomware variants</li><li>14. Confirm cybersecurity insurance coverages</li><li>15. Conduct ransomware simulations</li><li>16. Conduct phishing simulations</li><li>17. Conduct user awareness training</li><li>18. Conduct response training (this PBC)</li></ol>	<ol style="list-style-type: none"><li>1. Monitor for:<ol style="list-style-type: none"><li>a. Ransomware notes/messages</li><li>b. Unusual file extensions or malicious extensions</li><li>c. User reports of files being corrupt or not readable</li><li>d. Emails with suspicious attachments</li><li>e. Unusual DNS traffic</li><li>f. High velocity renaming of files</li><li>g. CPU spikes on file sharing systems</li><li>h. Unusual userland executable binaries</li><li>i. Anomalous network connections on hosts</li><li>j. Firewall denies to well known file sharing ports</li><li>k. Network connections to known C2 and exploit kit locations</li><li>l. Use of TOR or I2P</li></ol></li><li>2. Investigate and clear ALL alerts of possible ransomware<ol style="list-style-type: none"><li>a. IDS/IPS</li><li>b. Antivirus/EDR</li><li>c. Threat intelligence</li><li>d. Deception technology</li></ol></li></ol>	<ol style="list-style-type: none"><li>1. Inventory (enumerate &amp; assess)</li><li>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</li><li>3. Observe -&gt; Orient -&gt; Decide -&gt; Act</li><li>4. Locate and isolate the assets responsible for encrypting files</li><li>5. Isolate impacted file sharing systems</li><li>6. Close the attack vector</li><li>7. Fortify non-impacted file sharing systems</li><li>8. Fortify non-impacted critical assets</li><li>9. Issue perimeter enforcement for known threat actor locations</li><li>10. Deploy EDR hunter/killer agents and terminate offending processes</li></ol>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none"><li>1. Close the attack vector</li><li>2. Patch asset vulnerabilities</li><li>3. Re-image impacted assets</li><li>4. Inspect all assets for IOC consistent with the attack profile</li><li>5. Inspect user activity for IOC consistent with the attack profile</li><li>6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery</li><li>7. Implement newly obtained threat signatures</li></ol>	<ol style="list-style-type: none"><li>1. Restore to the RPO within the RTO</li><li>2. Restore from known clean backups</li><li>3. Address collateral damage</li></ol>	<ol style="list-style-type: none"><li>1. Perform routine cyber hygiene due diligence</li><li>2. Engage external cybersecurity-as-a-service providers and response professionals</li><li>3. Avoid opening email and attachments from unfamiliar senders</li><li>4. Avoid opening email attachments from senders that do not normally include attachments</li></ol> <div>Notes:<ol style="list-style-type: none"><li>1. Report cybercrime: <a href="https://www.ic3.gov/default.aspx">https://www.ic3.gov/default.aspx</a></li><li>2. Paying ransoms is discouraged but should be a contingency available to executives (SEE Preparation #12)</li></ol></div>



# Implementation

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



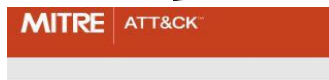
AV-CIRT-PBC-Template

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
- Provide Exec Summary
- 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

<b>SYNOPSIS</b>	1 NAME
Computer Incident Response Team Playbook Battle Card	2 SYNOPSIS
<b>SCOPE</b>	3 SCOPE
This instruction is intended for team members responsible for	4 DESCRIPTION
<b>DESCRIPTION</b>	4.1 Prologue
<b>Prologue</b>	4.1.1 Overview
<b>Overview</b>	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 <a href="https://github.com/certsocieteg">https://github.com/certsocieteg</a>	4.3.3 Create A GitHub Pull Request
	5 EXAMPLES
	6 NOTES / BUGS
	7 AUTHOR(S)
	8 REVIEWER(S)
	9 SEE ALSO

### 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.org/techniques/>

DESCRIPTOR = SHS INITCAP(ALPHA|SP)\* ; Ransomware; OPTIONAL industry/layman term

## AVAILABLE TO THE PUBLIC

[https://github.com/avertere\\_k12/avertere\\_soc\\_cirt-playbook-battle-cards](https://github.com/avertere_k12/avertere_soc_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

 <a href="#">images</a>	Brewing updates	5 hours ago
 <a href="#">GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf</a>	Brewing updates	5 hours ago
 <a href="#">LICENSE</a>	Initial commit	14 hours ago
 <a href="#">README.md</a>	Brewing updates	5 hours ago

 [README.md](#) [Edit](#)

A collection of Cyber Incident Response Playbook Battle Cards



(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none"> <li>1. Patch asset vulnerabilities</li> <li>2. Perform routine inspections of controls/weapons</li> <li>3. Examine file shares for loose/open privileges</li> <li>4. Maintain Antivirus/EDR application updates</li> <li>5. Create network segmentation</li> <li>6. Log traffic between network segments</li> <li>7. Incorporate threat intelligence</li> <li>8. Incorporate deception technology</li> <li>9. Perform routine inspections of asset backups</li> <li>10. Validate proper functionality</li> <li>11. Confirm backups are free of malware</li> <li>12. Establish ability to pay ransoms w/cryptocurrency</li> <li>13. Obtain decryption keys for ransomware variants</li> <li>14. Confirm cybersecurity insurance coverages</li> <li>15. Conduct ransomware simulations</li> <li>16. Conduct phishing simulations</li> <li>17. Conduct user awareness training</li> <li>18. Conduct response training (this PBC)</li> </ol>	<ol style="list-style-type: none"> <li>1. Monitor for:               <ol style="list-style-type: none"> <li>a. Ransomware notes/messages</li> <li>b. Unusual file extensions or malicious extensions</li> <li>c. User reports of files being corrupt or not readable</li> <li>d. Emails with suspicious attachments</li> <li>e. Unusual DNS traffic</li> <li>f. High velocity renaming of files</li> <li>g. CPU spikes on file sharing systems</li> <li>h. Unusual userland executable binaries</li> <li>i. Anomalous network connections on hosts</li> <li>j. Firewall denies to well known file sharing ports</li> <li>k. Network connections to known C2 and exploit kit locations</li> <li>l. Use of TOR or I2P</li> </ol> </li> <li>2. Investigate and clear ALL alerts of possible ransomware               <ol style="list-style-type: none"> <li>a. IDS/IPS</li> <li>b. Antivirus/EDR</li> <li>c. Threat intelligence</li> <li>d. Deception technology</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>1. Inventory (enumerate &amp; assess)</li> <li>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</li> <li>3. Observe -&gt; Orient -&gt; Decide -&gt; Act</li> <li>4. Locate and isolate the assets responsible for encrypting files</li> <li>5. Isolate impacted file sharing systems</li> <li>6. Close the attack vector</li> <li>7. Fortify non-impacted file sharing systems</li> <li>8. Fortify non-impacted critical assets</li> <li>9. Issue perimeter enforcement for known threat actor locations</li> <li>10. Deploy EDR hunter/killer agents and terminate offending processes</li> </ol>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none"> <li>1. Close the attack vector</li> <li>2. Patch asset vulnerabilities</li> <li>3. Re-image impacted assets</li> <li>4. Inspect all assets for IOC consistent with the attack profile</li> <li>5. Inspect user activity for IOC consistent with the attack profile</li> <li>6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery</li> <li>7. Implement newly obtained threat signatures</li> </ol>	<ol style="list-style-type: none"> <li>1. Restore to the RPO within the RTO</li> <li>2. Restore from known clean backups</li> <li>3. Address collateral damage</li> </ol>	<ol style="list-style-type: none"> <li>1. Perform routine cyber hygiene due diligence</li> <li>2. Engage external cybersecurity-as-a-service providers and response professionals</li> <li>3. Avoid opening email and attachments from unfamiliar senders</li> <li>4. Avoid opening email attachments from senders that do not normally include attachments</li> </ol> <div data-bbox="1280 816 1879 958"> <p>Notes:</p> <ol style="list-style-type: none"> <li>1. Report cybercrime: <a href="https://www.ic3.gov/default.aspx">https://www.ic3.gov/default.aspx</a></li> <li>2. Paying ransoms is discouraged but should be a contingency available to executives (SEE Preparation #12)</li> </ol> </div>