INCIDENT RESPONSE PLAYBOOK

CCDC IR Guide

THE IR EQUATION

```
PENALTY REDUCTION = QUALITY IR REPORT × SPEED OF RESPONSE

Quality reports can reduce Red Team penalties by up to 50%
This is DIRECT SCORE RECOVERY
```

IR PHASES (3-MINUTE CYCLE)

Phase 1: DETECT (30 seconds)

- Notice the anomaly
- Initial assessment: What system? What type?
- Alert Captain

Phase 2: CONTAIN (90 seconds)

- Block attacker IP
- Disable compromised account
- Isolate if necessary
- **DO NOT** destroy evidence

Phase 3: ANALYZE (60+ seconds)

- Determine entry point
- Identify scope
- Find persistence

Phase 4: DOCUMENT (Ongoing)

- Timeline with timestamps
- Commands used
- Evidence collected

INCIDENT REPORT TEMPLATE

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
                    INCIDENT REPORT
```

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

INCIDENT ID: IR-[YYYYMMDD]-[##]
REPORTED BY: _____
DATE/TIME: _____

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
EXECUTIVE SUMMARY
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
[2-3 sentences: What happened, what was affected, current status]




■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
TIMELINE
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
[HH:MM] Initial detection - How was it discovered?
[HH:MM] Alert raised - Who was notified?
[HH:MM] Containment action - What was done?
[HH:MM] Analysis started - What was found?
[HH:MM] Remediation complete - What fixed it?
[HH:MM] Services restored - Verification?
```

QUICK CONTAINMENT COMMANDS

Block Attacker IP

```
# Linux
iptables -I INPUT -s ATTACKER_IP -j DROP

# Windows
New-NetFirewallRule -DisplayName "Block_Attacker" -Direction Inbound -RemoteAddress ATTACKER_IP -Action Block
```

Disable Account

```
# Linux
passwd -l compromised_user
usermod -L compromised_user

# Windows (Local)
Disable-LocalUser -Name "compromised_user"

# Windows (AD)
Disable-ADAccount -Identity "compromised_user"
```

Kill Malicious Process

```
# Linux
kill -9 <PID>
pkill -f "suspicious_process"

# Windows
Stop-Process -Id <PID> -Force
Stop-Process -Name "suspicious" -Force
```

Isolate System (Network)

```
# Block all traffic to/from host
iptables -I FORWARD -s COMPROMISED_IP -j DROP
iptables -I FORWARD -d COMPROMISED_IP -j DROP
```

EVIDENCE COLLECTION

Linux Evidence

```
# Running processes
ps auxf > /evidence/processes_$(date +%Y%m%d_%H%M).txt

# Network connections
netstat -antup > /evidence/network_$(date +%Y%m%d_%H%M).txt
ss -antup >> /evidence/network_$(date +%Y%m%d_%H%M).txt

# Recent files
find / -mmin -60 -type f 2>/dev/null > /evidence/recent_files_$(date +%Y%m%d_%H%M).txt

# User activity
last > /evidence/logins_$(date +%Y%m%d_%H%M).txt
cat /home/*/.bash_history > /evidence/bash_history_$(date +%Y%m%d_%H%M).txt

# Cron jobs
crontab -l > /evidence/cron_root_$(date +%Y%m%d_%H%M).txt
cat /etc/crontab >> /evidence/cron_system_$(date +%Y%m%d_%H%M).txt

# Hash suspicious file
md5sum /path/to/suspicious/file
sha256sum /path/to/suspicious/file
```

Windows Evidence

```
# Running processes
Get-Process | Export-Csv -Path C:\evidence\processes.csv

# Network connections
Get-NetTCPConnection | Export-Csv -Path C:\evidence\connections.csv

# Recent events
Get-WinEvent -LogName Security -MaxEvents 500 | Export-Csv -Path C:\evidence\security_events.csv

# Scheduled tasks
Get-ScheduledTask | Export-Csv -Path C:\evidence\tasks.csv

# Services
Get-WmiObject win32_service | Export-Csv -Path C:\evidence\services.csv

# Hash suspicious file
Get-FileHash -Path C:\path\to\file -Algorithm SHA256
```

COMMON INCIDENT SCENARIOS

Scenario 1: Credential Compromise

```
DETECT: Failed login spike followed by successful login
CONTAIN: Disable account, reset password, block source IP
ANALYZE: Check what account accessed, lateral movement?
REMEDIATE: New passwords, enable MFA if possible, monitor
```

Scenario 2: Web Shell

```
DETECT: Suspicious POST requests, unusual file in webroot
CONTAIN: Remove file, block IP, restrict web directory
ANALYZE: Find upload vector, check for persistence
REMEDIATE: Patch upload vuln, verify no other shells
```

Scenario 3: Malware/Reverse Shell

```
DETECT: Unusual outbound connection, suspicious process
CONTAIN: Kill process, block C2 IP, isolate if needed
ANALYZE: Find execution source, check persistence
REMEDIATE: Remove malware, patch entry point
```

Scenario 4: Privilege Escalation

```
DETECT: Non-admin doing admin things, event 4672
CONTAIN: Disable account, check created accounts
ANALYZE: How did they escalate? Service exploit? Creds?
REMEDIATE: Patch vuln, rotate affected credentials
```

REPORT QUALITY CHECKLIST

Your IR report should answer:

- WHAT happened? (Clear description)
- WHEN did it happen? (Accurate timeline)
- WHERE did it happen? (Systems/services affected)
- HOW did it happen? (Attack vector)
- WHO was involved? (Attacker IPs, accounts)
- WHAT did you do? (Containment actions)
- WHAT's the impact? (Business effect)
- WHAT will prevent recurrence? (Recommendations)

PENALTY REDUCTION GUIDE

Report Quality	Penalty Reduction
No report	0%
Basic (what happened)	10%
Good (timeline + containment)	25%
Excellent (full analysis + recommendations)	50%

What Makes "Excellent"

- Precise timestamps (HH:MM:SS)
- Specific technical details (IPs, ports, commands)
- Evidence references (log lines, hashes)
- Clear containment actions
- Root cause identified
- Prevention recommendations

IR MANTRA

> *""CONTAIN in 3 minutes."*
>
> *"DOCUMENT everything."*
>
> *"QUALITY reports = SCORE recovery.""*

CCDC.x1000.ai - Championship Training