InfraGard
Partnership for Protection

INCIDENT RESPONSE TEMPLATES

Get Started

Pick the detail level that works right for you. Remember that these are just frameworks. Your organization will have it's own unique considerations and you should tailor your plan to those needs.

Executive Template

Analyst Template

INFRAGARD ALBANY MEMBERS ALLIANCE

infragardalbany.org

InfraGard
Partnership for Protection

Executive Template

- [ ] **Preparation**
  - [ ] What happened?
  - [ ] If the adversary is known to us, do we have indicators available?
  - [ ] What does the adversary want?
  - [ ] What does the adversary already have?
  - [ ] Do other teams or law enforcement need to be integrated into the response?
  - [ ] Have we evaluated the need to have a third party response team involved?
  - [ ] What are we most concerned about losing?
    - [ ] Is it possible to easily isolate or protect that data (segregation, encryption, access controls)?
    - [ ] If the concern is ransomware, do we have backups? Are the backups at risk?
  - [ ] What other control implementation points exist (Firewall, Endpoint Protection, Intrusion Prevention System?)
  - [ ] Have we alerted any relevant stake-holders?
  - [ ] **Implement identification phase without blackholing, blocking or prematurely isolating**

- [ ] **Identification and Scoping**
  - [ ] **Initial response**
    - [ ] Implement crown jewel protection if possible
    - [ ] Are any machines already identified as problematic via system alerts?
    - [ ] Utilize endpoint collection agents on suspect machines if available
    - [ ] **Begin thorough network monitoring**
      - [ ] **PCAPs and Netflow Analysis**
    - [ ] **Triage Collection on suspect devices**
    - [ ] **Memory Analysis**
    - [ ] **Triage Timeline**
    - [ ] **Incident assessment** - Updated Daily until Remediation Complete
      - [ ] Once Daily
    - [ ] **Additional indicator creation** - Updated Twice Daily until Identification/Scoping Complete
      - [ ] First Update
      - [ ] Second Update

- [ ] **Deep dive**
  - [ ] Establish team parameters for threat hunting
  - [ ] File System Analysis - Semi Automated
  - [ ] Anti-forensic detections
  - [ ] File System Analysis - Manual
  - [ ] Adversary profiling
    - [ ] Does our adversary's IP range, domain info, tools, attack timing, behavior or victim selection indicate a specific threat actor?
  - [ ] Define threat capabilities and purpose
  - [ ] Additional indicator creation

- [ ] **Containment and Remediation** - DO IN ORDER
  - [ ] Apply all current Indicators to enterprise monitoring tools, construct list of known compromised hosts.
  - [ ] Disconnect network from internet
  - [ ] Implement network segmentation if possible
  - [ ] Block malicious IP addresses
  - [ ] Blackhole bad domains
  - [ ] Remove and re-image all infected systems > If forensic images are required for Law Enforcement, make those before destroying evidence
  - [ ] If needed, remove all systems identified as compromised
  - [ ] Cloud and Service coordination
  - [ ] Enterprise password change
  - [ ] If compromise relied on a vulnerability, patch vulnerability
  - [ ] Verify that these steps each actually happened

- [ ] **After Action**
  - [ ] Report
  - [ ] Stakeholder follow-up
  - [ ] Partner follow-up (if other relevant partners, law enforcement teams were not part of follow-up)

InfraGard
Partnership for Protection

Analyst Template

- [ ] **Preparation**
  - [ ] What happened?
  - [ ] If the adversary is known to us, do we have IOC's available?
  - [ ] If attack was reported via SOC or third party, can they share what infrastructure alerted them?
  - [ ] If attack was reported via stakeholder, do we have an established POC with the victim? If not, who are the best people at the agency to meet for notification?
  - [ ] If the concern is DDOS, skip to DDOS Response Policy
  - [ ] Incident Survey
    - [ ] **Incident Background**
      - [ ] What is the nature of the problem, as it has been observed so far?
      - [ ] How was the problem initially detected? When was it detected and by whom?
      - [ ] What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)
      - [ ] What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?
      - [ ] What groups or organizations were affected by the incident? Are they aware of the incident?
      - [ ] Were other security incidents observed on the affected environment or the organization recently?
    - [ ] **Communication Parameters**
      - [ ] Which individuals are aware of the incident? What are their names and group or company affiliations?
      - [ ] Who is designated as the primary incident response coordinator?
      - [ ] Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)
      - [ ] What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?
      - [ ] What is the schedule of internal regular progress updates? Who is responsible for them?
      - [ ] What is the schedule of external regular progress updates? Who is responsible for leading them?
      - [ ] Who will conduct “in the field” examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.
      - [ ] Who will interface with legal, executive, public relations, and other relevant internal teams?
    - [ ] **Incident Scope**
      - [ ] What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?
      - [ ] What applications and data processes make use of the affected IT infrastructure components?
      - [ ] Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)
      - [ ] What are the possible ingress and egress points for the affected environment?
      - [ ] What theories exist for how the initial compromise occurred?

- [ ] Does the affected IT infrastructure pose any risk to other organizations?
- [ ] **Incident Survey Review**
  - [ ] What analysis actions were taken to during the initial survey when qualifying the incident?
  - [ ] What commands or tools were executed on the affected systems as part of the initial survey?
  - [ ] What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)
  - [ ] What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)
  - [ ] If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?
- [ ] **Planning the Response**
  - [ ] Has law enforcement been notified? Can they provide additional indicators?
  - [ ] Is there a third party IR team involved?
  - [ ] Does the affected group or organization have specific incident response instructions or guidelines?
  - [ ] What are the victim's crown jewels?
    - [ ] Is it possible to easily isolate or protect that data (segregation, encryption, access controls)?
  - [ ] What does the adversary want, if known?
  - [ ] What does the adversary already have, if known?
  - [ ] What tools are available to us for monitoring network or host-based activities in the affected environment?
  - [ ] What initial IOC's does the victim have available?
  - [ ] What IOC implementation points exist (Firewall, AV, IPS) (these may be the same as network monitoring points)
  - [ ] Where are the affected IT infrastructure components physically located?
  - [ ] What backup-restore capabilities are in place to assist in recovering from the incident?
  - [ ] Are there any enterprise collection capabilities (Encase, F-Response, etc).
  - [ ] What mechanisms exist for transferring files for analysis (ftp server, cloud, in person pickup, etc)
  - [ ] Do you have any baselined- for-sure-not-infected-boxes, for baseline memory comparison?
  - [ ] **Implement identification phase without blackholing, blocking or prematurely isolating**

Identification and Scoping

- [ ] **Initial response**
  - [ ] Are any boxes already identified as problematic via callouts, IDS or AV alerts?
  - [ ] Import IOC's into triage tools
  - [ ] Import IOC's into network monitors, such as firewalls, IDS or custom Snort instance
  - [ ] Import IOC's into a custom malware scanner like Clam or Yara
  - [ ] Implement crown jewel protection if possible
  - [ ] Enterprise collection capabilities - if there are any in play, use them as available to facilitate collection across multiple devices
  - [ ] **PCAPs and Netflows**
    - [ ] If there are no PCAP collections in place, is it possible to implement a listener?

- [ ] Review collections at a reasonable interval once collection has started.
- [ ] If there is a PCAP, review with Snort, Wireshark. If the PCAP is huge, consider converting that to netflow with nfdump's nfpcapd utility (or restreaming DNS with tshark), then attacking the netflow.
  - [ ] Convert pcap to netflow
    - [ ] Consider converting that output to csv for review or database ingest
  - [ ] Snort - Custom IDS
    - [ ] Snort -c /etc/snort.conf -K ascii -l -log -r example.pcap
      - [ ] Run snort against current ruleset. Make sure ruleset has been updated to reflect IOCs.
    - [ ] Grep '\[**'alert | wc -l
      - [ ] How many alerts do we have?
    - [ ] Grep '\[**'alert | sort | uniq -c | sort -rn > sorted_alerts.txt
  - [ ] PassiveDNS - quickly pull DNS queries out of a pcap
  - [ ] Wireshark – look at hierarchy, top and bottom talkers, suspect ports

- [ ] **Triage Collection on suspect devices**
  - [ ] Have all appropriate authority to go hands on with target
  - [ ] Considered implications of triaging method against potentially attacker monitored machine
  - [ ] Kick off a memory image (see win32/64, redline collector, volatility's winpmem, linpmem, macpmem or FTK imager)
  - [ ] Redline Autoruns and IOC collector (be careful with options, can be very slow with too much)
    - [ ] Live Forensics Checklist (if conducting on-the-box analysis)
      - [ ] Unusual Network Usage
        - [ ] c:\> net view \\127.0.0.1 (looking for file shares and make sure each has a purpose)
        - [ ] c: net session (look at who has an open session with machine)
        - [ ] c: net use (look at which sessions this machine has opened with other systems
        - [ ] c: nbtstat -S (look at NetBIOS over tcp/ip activity)
        - [ ] c: netstat -na (look for unusual listening tcp/udp ports)
        - [ ] c: netstat -na 5 (continuous polling)
        - [ ] c: netstat -naob (o flag adds PID, b flag shows exe and associated dll's)
        - [ ] Xp/2003 C: netsh firewall show config
        - [ ] Win7+ c: netsh advfirewall show currentprofile
      - [ ] Unusual Processes (hard to do from cmd prompt, focus on networked items or get a basic list and move on until volatility)
        - [ ] c: Tasklist
        - [ ] c: wmic process get name, parentprocessid, processid
        - [ ] c: wmic process where processid=<PID> get commandline
      - [ ] Unusual Services (hard to do from cmd prompt, focus on services related to any suspect process or IOC, then move on until Redline or Volatility)
        - [ ] c: services.msc (anything running with just user privs?)

- [ ] c: tasklist /svc (if you have an IOC or suspect process in mind)
- [ ] Unusual Registry (again, Autoruns or Redline would be more optimal, but if you have time to kill)
  - [ ] Regedit for autostart locations under deepdive>malware
  - [ ] c: reg query hklm\software\microsoft\windows\currentversion\run
  - [ ] Don't forget hkcu too
- [ ] Extra Startup Points:
  - [ ] Msconfig
  - [ ] Xp: c: dir /s /b "C:\Documents and Settings\username\Start Menu\"
  - [ ] Win7: c: dir /s /b "C:\Users\username\Start Menu\"
- [ ] Unusual Accounts
  - [ ] Lusrmgr.msc (click groups, double click administrators)
  - [ ] c: net user
  - [ ] c: net localgroup administrators
- [ ] Big files (warning, recursive scanning for big things might take some time, but the bigger the less hits)
  - [ ] c: FOR /R C:\ %i in (*) do @if %~zi gtr 10000000 echo %i %~zi
  - [ ] Strongly consider an output file if you do that.
- [ ] Scheduled tasks
  - [ ] Open task scheduler / scheduled tasks, look for ones by administrators, system, or blank
  - [ ] c: at (only shows at tasks, if any, for the lazy hacks)
- [ ] Cursory Log Analysis
  - [ ] ps: Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624,4625,4672,4720,4722,4724,4732,4738,4776,4778,4779,5140,1102}
  - [ ] Ps: Get-WinEvent -FilterHashtable @{LogName="System"; ID=7030,7045,1056,10000,100001,10100,20001,20003,24576,24577,24579} (warning, may need output file)
  - [ ] Ps: Get-WinEvent -FilterHashtable @{LogName="Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"; ID=2003}
  - [ ] Ps: Get-WinEvent -FilterHashtable @{LogName="Application"; ID=11707,11724}
  - [ ] ***What other events should get exported?

- [ ] **Memory Analysis**
  - [ ] Redline
    - [ ] What processes have super high MRI (requires version 1.1) and why?

- [ ] What are their parent processes?
- [ ] What user account SIDs spawned the process?
- [ ] What is the binary path of the processes?
- [ ] Is anything else of interest in this binary path (may require mounting in FTK imager or manually looking to see content in notepad or hexedit)?
- [ ] View hierarchal process list. Is anything else spawned from the same parent? If so, repeat previous steps.
- [ ] View the handles tab for each suspect process, sorting handles by least occurrence, and note suspect handles.
- [ ] View the loaded DLL for each suspect process (section tab), and sort by least occurrence, and note suspect handles.
- [ ] View the Ports list. Note any suspect connections and the processes that spawned them. If these are new processes, repeat above steps.
- [ ] View the strings list. Search for ftp, exe, c:\, urls, http, https, IP patterns.
- [ ] Build additional IOC's from these results.
- [ ] **Injection Button?

- [ ] Volatility - See Volatility Cheat Sheet(s) for command flags. vol.py -f image --profile=profile plugin.
  - [ ] Imagecopy any additional recovered crash or hibernation files
  - [ ] Imageinfo to secure your profile, grab the kdbg number
    - [ ] Note: windows8 / 2012 and newer rely on kdcopyblock, not kdbg. This is found using vol.py -f mem.dmp kdbgscan.
  - [ ] Rogue Processes
    - [ ] Compare pslist (lists processes) to psscan (carves processes) for differences with pstotal
    - [ ] Pstree to find parents of bad children
      - [ ] Sanity check that the process are what they report to be
    - [ ] Malsysproc (looks for bogus system processes)
    - [ ] Baseline (compare to a baseline if one was available
    - [ ] Servicebl (compare to a baseline if one was available
  - [ ] Network Artifacts
    - [ ] XP: connections, connscan, sockets
    - [ ] Win7+: netscan
  - [ ] Code Injection
    - [ ] Malfind for injected code
    - [ ] Ldrmodules for unlinked DLLs
  - [ ] Rootkit Check
    - [ ] ***Psxview (this is pslist vs psscan + several other plugins)
    - [ ] Modscan (walks kernel drivers)
    - [ ] Ssdt

- [ ] apihooks
- [ ] DLL and Handles
  - [ ] Dlllist
  - [ ] Getsids
  - [ ] Handles
  - [ ] Svcscan (use -v parameter, difficult to eyeball bad drivers)
- [ ] Dump Suspect Processes and Drivers
  - [ ] Dlldump (dlls)
  - [ ] Moddump (kernel drivers)
  - [ ] Procdump (process dump)
  - [ ] Memdump (for memory captures, but you could dump just a specific processes memory for strings or file extract with -p)
    - [ ] Strings and grep the memdump of the process
  - [ ] Dumpfiles (files)
  - [ ] Filescan (similar to dump files, but carves)
- [ ] Bonus: Registry Analysis from memory! Not always needed if you pulled the registry, but some key changes aren't saved till restart, or maybe you didn't get to pull the registry yet.
  - [ ] Registry
  - [ ] Autoruns
  - [ ] USN Journal Entries
  - [ ] Ethscan network packets
  - [ ] Mimikatz passwords
  - [ ] Firefoxhistory (works for chrome too)
- [ ] If you found malware, send a copy to a sandbox and compare against public AV libraries and OSINT. Full analysis later if you don’t have a "known" sample.
- [ ] Build additional IOC's from these results

- [ ] **Triage Timeline**
  - [ ] Find execution times of malware, remote access tools and psexec. PSExec on the source, PSEXESVC on the target.
  - [ ] Prefetch - first and last executes, from comprehensive collect or vol prefetchparser plugin
  - [ ] AppCompat/Shim; requires SYSTEM or mem. Mem may be better since Shim is only written to registry on reboot! Likely wont net an execution time, but may show an execution you needed to prove or track down.
    - [ ] Shimcacheparser.py
    - [ ] Vol shimcachemem
    - [ ] Win7: Recentfilecache.bcf ; c:windows\appcompat\programs, rfc.pl
    - [ ] Win7/8/10: Amcache.hve; gives first execute time; same location as recent file cache

- [ ] VSS versions of prefetch / AppCompat - obviously requires full disk access. Useful step if you want to verify IOC presence in older backups
  - [ ] Mounting VSS
- [ ] Investigate lateral movement - This phase can become "deep dive" too, so leave time for daily incident assessment updates and new IOC writeups.
  - [ ] Event logs - Outside of Redline collector, some of these events were collected by powershell scripts earlier in Triage. Numbers below are event ID's.
    - [ ] Log Tampering
      - [ ] 1102 - audit log cleared (Security log)
      - [ ] 104 - audit log cleared (System log)
    - [ ] Local account authorization
      - [ ] 4776 - or 4768 in Kerberos
      - [ ] 4672 - privileged account use, possible local admin escalation
    - [ ] Unexplained accounts
      - [ ] 4720 - account creation
    - [ ] Weird timing
      - [ ] 4624 - logon
      - [ ] 4634 / 4647 - logoff (logoffs are not well recorded)
    - [ ] Remote Logons
      - [ ] 4624 type 10 (rdp) or type 2 (vnc or psexec -u) or type 3 (psexec) on target system
      - [ ] 4625 failed logons, guesses or brute force
        - [ ] Or 4771 in kerberos
      - [ ] 4778/4779 rdp session events on target system. Also check TerminalServices_RemoteConnectionManager.evtx (1149 (successful RDP connection))
      - [ ] Application logs for teamviewer and vnc -- we capture installation but not use in scripts, may require deep dive or comprehensive redline collector
      - [ ] RemoteDesktopServices-RdpCoreTS (event ID 131 and 98)
      - [ ] Microsoft-Windows-TerminalServices-LocalSessionManager
      - [ ] TaskScheduler event 119
      - [ ] Tying logins together if dealing with multiple boxes
    - [ ] Strange app installs Application log
      - [ ] 1033, 11707 - install (1033 will have a success or failure flag)
      - [ ] 1034, 11724 - uninstall (1034 will have a success or failure flag)
      - [ ] 11708 - install failure
    - [ ] Windows Admin Share use
      - [ ] 4624 type 3 (target system)
      - [ ] 4672

- [ ] 5140 network share access (target system) (may also indicate psexec on target) (requires audit of file share enabled in GPO)
- [ ] Task Scheduler
  - [ ] Task created 106 | 4698 (Task Scheduler | Security)
  - [ ] Task executed 200-201 (Task Scheduler)
- [ ] Services
  - [ ] 7036 - service start, can return a ton of hits - System
  - [ ] 7045 - service installed - System
  - [ ] 4697 - service installed - Security
- [ ] Microsoft Antimalware log event 1006
- [ ] Process Tracking is rarely enabled, but look for event 4688 in security. Can return overwhelming amount of hits, but hits on newer systems may include process command line (released server 2012 and backported to windows7)
- [ ] Powershell logging (if enabled) - PowerShell/Operational log
  - [ ] 4104 script contents
  - [ ] 4105/4106 script start/stop

- [ ] Registry
  - [ ] Ntuser\software\microsoft\terminal server client\servers (and *\default) (rdp use on source)
  - [ ] Ntuser\software\microsoft\windows\currentversion\explorer\mountpoints2 (share use on source)
  - [ ] System\currentcontrolset\services\psexesvc (psexec targets)
  - [ ] Ntuser\software\sysinternals\psexec\eulaaccepted (psexec source, 1st time only)
- [ ] Memory
  - [ ] Was Psexec, psexesvc, teamviewer, vnc or other remote access tool in memory? (use the handles function of redline or volatility, cmdscan or svcscan)
- [ ] Filesystem
  - [ ] In addition to Psexec and psexesvc, was there any evidence of wmiprvse, powershell and wsmprovhost in prefetch, shim or appcompat? These latter items may indicate powershell remoting/wmic.

- [ ] Timeline out in Excel the who / what / where / when of every suspect event identified in previous stage:
  - [ ] Execution
  - [ ] Process
  - [ ] Service
  - [ ] Task
  - [ ] Registry entry
  - [ ] Lateral movement trace
- [ ] Begin a full image if Deep Dive analysis will be required for this device.

- [ ] Begin triage on other targets if later movement was detected or IOC scans have detected other potentially compromised hosts.
- [ ] **Incident assessment** - Updated Daily until Remediation Complete
  - [ ] Once Daily
- [ ] **Additional indicator creation** - Updated Twice Daily until Identification/Scoping Complete
  - [ ] First Update
  - [ ] Second Update

- [ ] **Deep dive - Steps below generally require an image**
  - [ ] Battleplan
    - [ ] Consider time constraints verse team resources
    - [ ] Consider current discoveries verse quantity of suspected compromised hosts.
    - [ ] If you are light on triage discovery, full file system analysis may be prudent. If you are heavy on triage discovery, it may cost the victim time better spent moving to Containment.
    - [ ] If you have a team (including victim's IT folks if proficient), can timelining, malware hunting, manual malware analysis be split among pros to move faster?
  - [ ] File System Analysis - Semi Automated
    - [ ] **Super Timelining** - This is the most time intensive step on the entire list short of creating and processing an image. Supertimelines are a useful preparing step for malware hunting if you don't believe you have identified all the artifacts yet, and for a detailed final report.
      - [ ] Utility choice
        - [ ] IEF/AXIOM Timeline can quickly filter most* of the events we want in a timeframe we want. Processing a case is similar to FTK wait times. Can export results to a log2timeline formatted csv. *Warning: parses files in predetermined categories, exe's and non standard extension types are excluded unless they show up somewhere else, like prefetch, shellbags or userassist.
        - [ ] Log2timeline - The free option. Processing a case is similar to FTK wait times, but easier for incorporating into a written report and bash parsing than IEF because it defaults to excel output.
        - [ ] MFT2CSV - This timeline is the fastest way to do things and will probably miss half the artifacts without per-file comparison. Do this if you are stuck waiting for something to process or incorporate into triage phase for faster finds from MFT.
        - [ ] FLS - Also very fast. Pulls from a few more sources than MFT2CSV, including the registry, inodes.
  - [ ] Anti-forensic detections
    - [ ] Log cleared entries
    - [ ] Timestomper
    - [ ] Secure erase tools

- [ ] File System Analysis - Manual
  - [ ] Malware Hunting
    - [ ] Autostart locations (use tools: regripper, autoruns, kansa)
      - [ ] NTUser.dat\software\microsoft\windows\currentversion\run
      - [ ] *\runonce
      - [ ] Software\microsoft\windows\currentversion\run
      - [ ] *\runonce
      - [ ] *\policies\Explorer\run
      - [ ] Software\microsoft\windows NT\currentversion\winlogon\userinit
      - [ ] %appdata\roaming\microsoft\windows\start menu\programs\startup
    - [ ] Service Creation / Replacement
      - [ ] (use tools: autoruns, windows "SC" cmd
    - [ ] Service Failure Recovery
      - [ ] (use tools: kansa powershel script Get-SvcFail.ps1)
    - [ ] Scheduled Tasks - (jobparser.py, jobparse.pl)
      - [ ] Look for "at" and "schtasks" execution
      - [ ] Windows\tasks
      - [ ] Windows\system32\tasks
      - [ ] Task Scheduler Operation evtx
    - [ ] DLL Hijack
      - [ ] DLLs outside system32 or in same folder as exe, ntshrui.dll
      - [ ] Phantom dll hijacking, loading dll's that don’t exist in modern windows, fxsst.dll
      - [ ] DLL sideloading, loading in SxS, PlugX
    - [ ] WMI Event Consumers
      - [ ] IFTTT for events. Autoruns, Kansa detect this. Powershell "Get-WmiObject" can also be used natively.
    - [ ] Advanced
      - [ ] Weird group policies
      - [ ] MS Office add-ons
      - [ ] BIOS flashing/hardware compromise
      - [ ] Deleted files
      - [ ] Unexplained encrypted containers
    - [ ] If not found, roll through SANS DFIR Find Malware / Windows Forensic Analysis poster artifact types one at a time with a filter for your chosen timeline utility that isolates those artifacts, flagging each item that is relevant to the timeline for review
  - [ ] Malware Analysis
    - [ ] See Malware Analysis Cheat Sheet v1 and v2, REMnux Usage Tips, Malicious Documents Cheat Sheet, and DFIR SIFT / REMnux guide as needed.
    - [ ] Sandbox if not done in Triage. Good sandboxes include:

- [ ] Malwr.com – if they're up...
- [ ] MCAP by MS-ISAC, requires registration and a human activation. (https://mcap.cisecurity.org/login)
- [ ] Hybrid Analysis / VXStream - some good features are behind a paywall
- [ ] For a list of other sandboxes, https://zeltser.com/automated-malware-analysis/

- [ ] Basic Static
  - [ ] AV scan and/or Virustotal
  - [ ] Hash value as an indicator
  - [ ] Strings
  - [ ] Packer detection (PEiD)
  - [ ] Dependency walking
  - [ ] PE File Headers
- [ ] Basic Dynamic
  - [ ] Regshot (clean shot, save for baseline)
  - [ ] Getting malware to run (for sandbox aware malware, try bare-metal analysis or debugging)
  - [ ] Procmon and Process Explorer
  - [ ] Compare strings between the image and memory
  - [ ] If you found a malicious DLL in memory analysis, use Process Explorer's dependency walker to see where else it might be used
  - [ ] Regshot (2nd shot comparison)
  - [ ] Faking a Network for DNS / IP callouts
- [ ] Advanced Static
- [ ] Advanced Dynamic

- [ ] Remote Access and Lateral Movement
  - [ ] Documents or My Documents: Default.rdp
  - [ ] If Psexec or WMIC use was found, parse application log for all of psexesvc service start and stop times
  - [ ] Remote updating services
  - [ ] Exploit use

- [ ] Adversary profiling
  - [ ] Does our adversary's IP range, domain info, tools, attack timing, behavior or victim selection indicate a specific threat actor?
- [ ] Define threat capabilities and purpose
  - [ ] Rate the TTP's used by the enemy on a scale of 1-10. Keep in mind high opportunity level of victim may only warrant use of low level TTP's.
  - [ ] What was the adversary's goal?
- [ ] Additional indicator creation

- [ ] **Containment and Remediation** - DO IN ORDER
  - [ ] Apply all current IOC's to Yara and IDS, construct list of known compromised hosts.
  - [ ] Disconnect network from internet – consider that some malware may self destruct and know what you are dealing with
  - [ ] Implement network segmentation if possible
  - [ ] Block malicious IP addresses
  - [ ] Blackhole bad domains – if no on-prem DNS, consider a temporary VM or Pi-Hole for this.
  - [ ] Remove and re-image all infected systems - If forensic images are required for Law Enforcement, make those before destroying evidence
  - [ ] If needed, remove all systems identified as compromised
  - [ ] Cloud and Service coordination
  - [ ] Enterprise password change if appropriate
  - [ ] If compromise relied on a vulnerability, patch vulnerability – with proper testing, if patch can be implemented in a non-detrimental way to the reliant software.
  - [ ] Verify that these steps each actually happened

- [ ] **After Action**
  - [ ] Report
    - [ ] Executive understandable summary
    - [ ] IOCs for Victim Intel team, partners and FBI intel
    - [ ] Detail of response processes that identified an artifact
  - [ ] Victim follow-up
    - [ ] Sell the hard work of victim team members in facilitating response – Prohibit blamestorming
    - [ ] Brief executive summary, future legal steps, benefits of continuous relationship
    - [ ] If APT, underscore reality of future compromise attempts
  - [ ] Partner follow-up (if other relevant teams were not part of follow-up)

Incident Survey Questions Credit to Lenny Zeltser at https://zeltser.com/

Other items were written by collaboration. Special thanks to the independent members of FBI, New York State Cyber Command, New York State DHSES, Center for Internet Security, SANS and IBM X-Force who took the time to help review items and provide feedback.

Tools and techniques are provided for example or reference and are not an endorsement.

Questions are designed as a checklist for handling an incident and do not include all considerations that should be made to secure an environment before or after an intrusion.