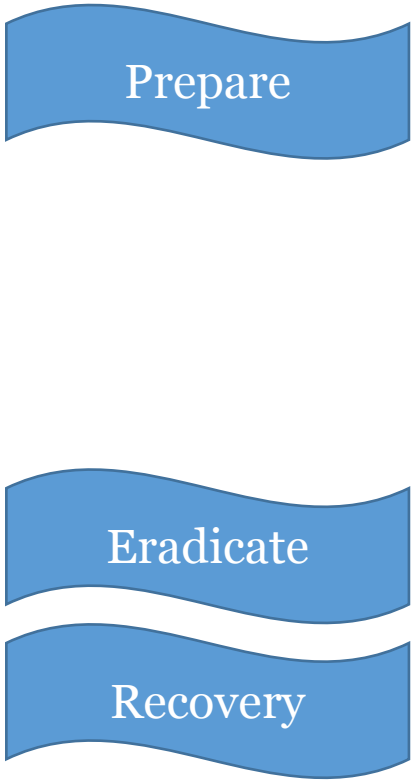
Slides taken from a private presentation

All notes will eventually make their way into SANS FOR528.
Requested via Twitter and pushed to GH to share ☺.

Ryan Chapman (@rj_chap)

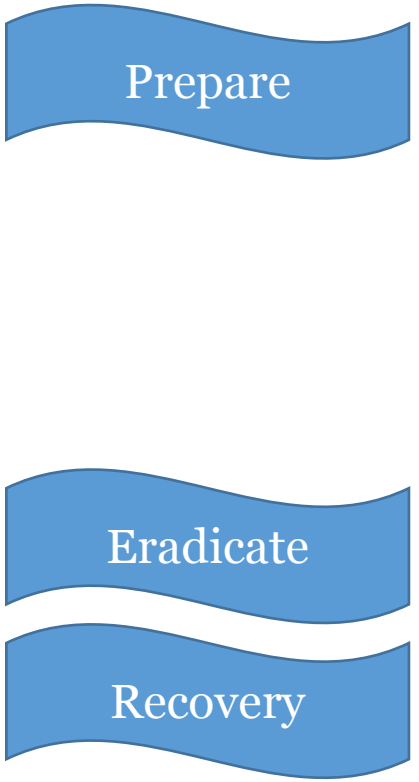
Disaster Recovery

- See "Surviving a Ransomware Attack with Azure Site Recovery"
- Setup Disaster Recovery Sites in Windows Admin Center
  - Ability to replicate VMs in another Azure region
- NEVER, EVER, EVER use "Planned Failover" for ransomware recovery
  - This option synchronizes the ransomed system – NOOOOO!!!!
- DISABLE replication to avoid overwriting snapshots
  - You may have ~24 hrs of backups in replication
- DO NOT check "Shut down and synchronize" when restoring
  - Basically the same as using "Planned Failover"



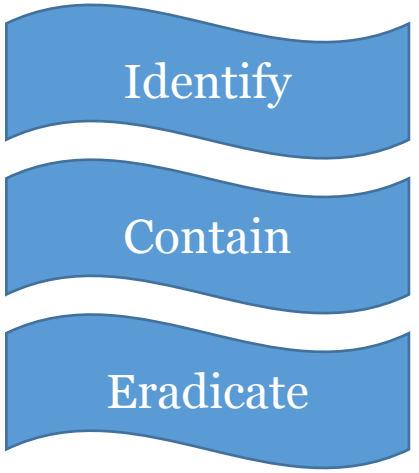
Azure Backup

- Azure Backup documentation
- Ability to set a PIN for critical operations
  - See 8:55 here in this video from Microsoft Mechanics for PIN setup
  - Ransomware/malware that attempts to remove Azure backups will *FAIL*!!
- Integration with 3rd party providers (e.g. Commvault)
- Think about using Immutable Blob Storage
  - See 6:06 here in this awesome video from Azure Ninjas (watch the whole thing!)
  - "Write Once, Read Many" (WORM) containers
  - Data can be written into it, but the data *cannot be modified*
  - Sorry, not sorry, ransomware ☺



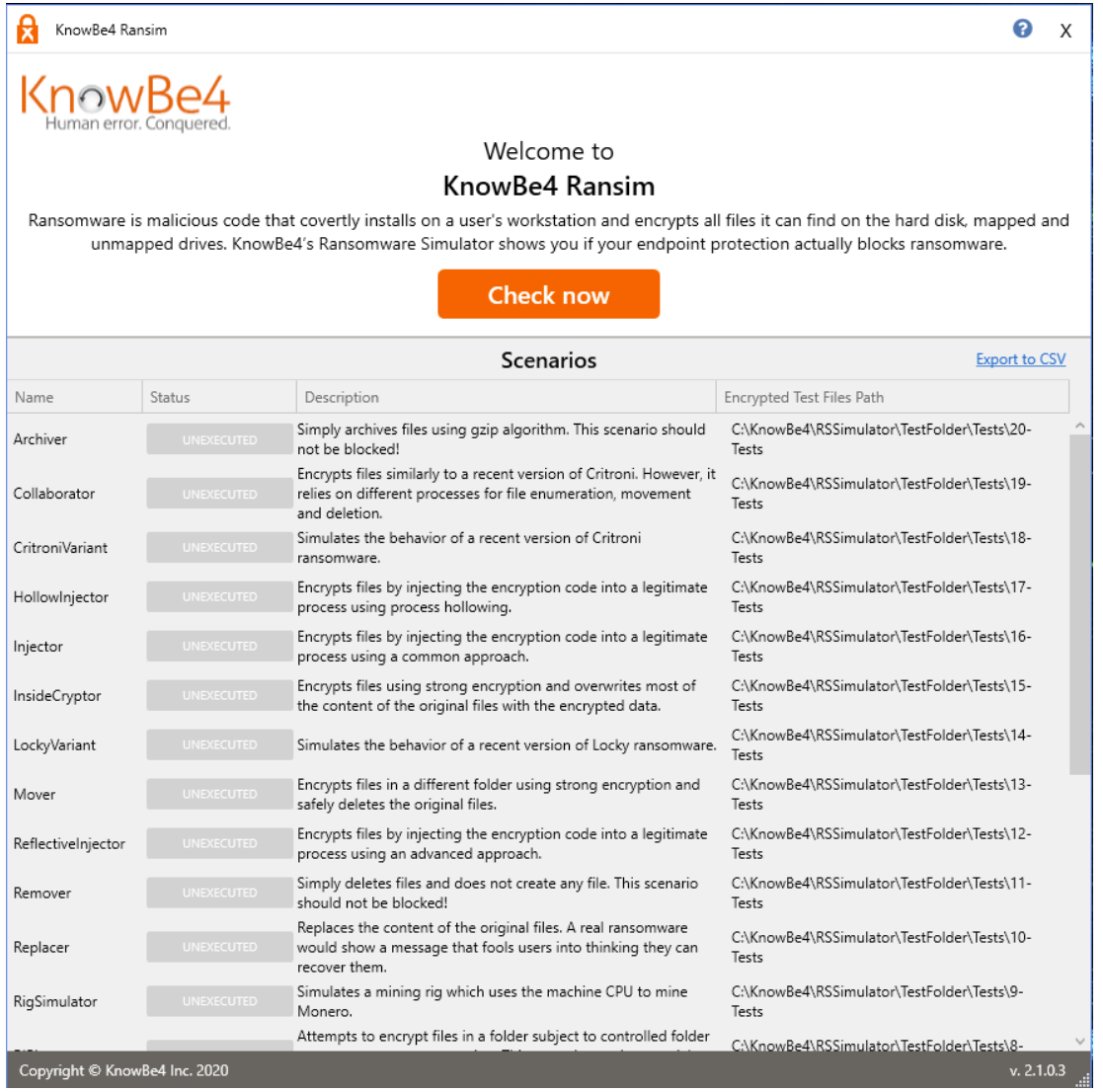
Ransomware is Running NOW!! cont.

- Your focus: Lateral movement activity
- Be on the lookout for common lateral movement activity
- Could be the Threat Actor, the ransomware, or both!
- Lookout for:
  - SMB, WMI, WinRM, and RDP
- See "Inside Microsoft Threat Protection: Attack modeling for finding and stopping lateral movement"



Azure Security Center

- Security Center
  - Check out the "Ransim" Ransomware Simulator by KnowBe4
- To test your Security Center alerting:
  - Download, install, and run Ransim
  - Review Security Center reports
  - Did *each* of the sections trigger an alert?
- Your AV/EDR
  - Are they missing any alerts?
  - Can you adjust them to catch it?



Azure Security Center cont.

- File Integrity Monitoring (FIM) can help detect ransomware running
  - Ransomware modifies/created files quickly
  - FIM is a key to identifying this type of activity
  - (External SIEMs can also monitor for file modifications btw)
- Security Center -> Advanced Cloud Defense -> File Integrity Monitoring

- Narendra Sahu has a great video detailing the setup
  - See 5:52 here

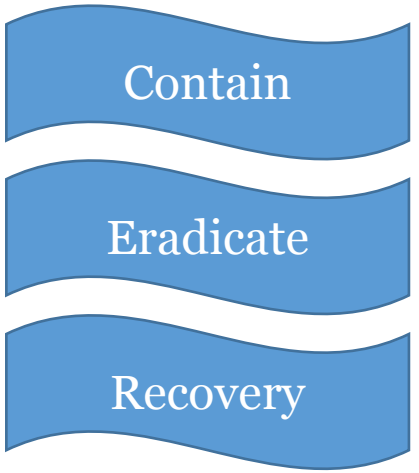
Azure Security Center Response

- Response actions

- Collect investigation package
  - A bunch of live response data
- Isolate the machine(s)
  - Speaks for itself ☺
- Network isolation documentation
  - If ransomware is spreading quickly, you may want to cut an entire network segment (or more)

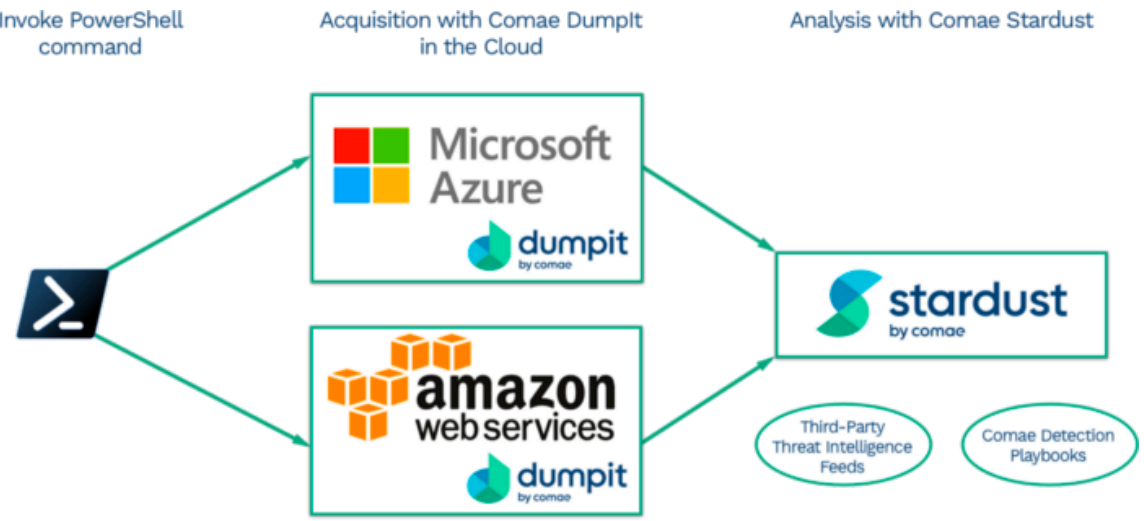
DFIR Tools in Azure

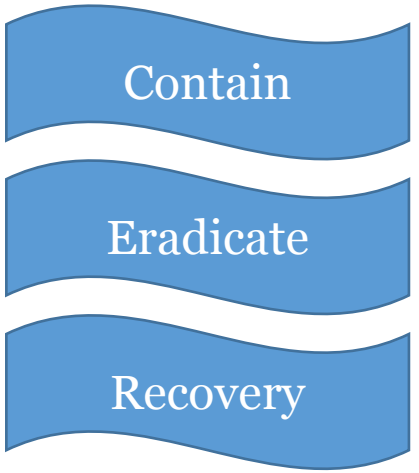
- Pulling forensic data in Azure can be… tricky…
- Built-in method digital forensic evidence harvesting:
  - General "Computer forensics in Azure" documentation
  - Copy-VmDigitalEvidence runbook
- Built-in memory capture:
  - Yeah, this method is LAME, as it requires pre-setup
  - If you don't pre-setup, you have to REBOOT the system to configure it
    - Purpose = defeated
  - See https://heranonazure.wordpress.com/2018/09/26/created-a-dump-for-a-running-vm-in-azure



DFIR Tools in Azure cont.

- Outside the built-in options, general DFIR tools do the job
- Memory capture tool recommended – DumpIt
  - See https://zeltser.com/memory-acquisition-with-dumpit-for-dfir-2/
  - Tested to work with Azure, including for Linux VMs





- See also: Hal Pomeranz's LMG script