STORAGE DEVELOPER CONFERENCE
SDC 21
BY Developers FOR Developers

Virtual Conference
September 28-29, 2021

A SNIA Event

Ransomware

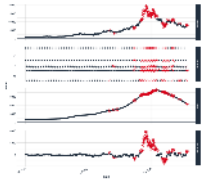
Detection, Mitigation, and Recovery

Chris Lionetti, HPE & SNIA Vice-Chair

Agenda : Plan of Attack

- Patch and Harden your Infrastructure

- Baseline and Ongoing Monitor



- Anomaly Analysis

- Isolation of the Infected, determine start of infection

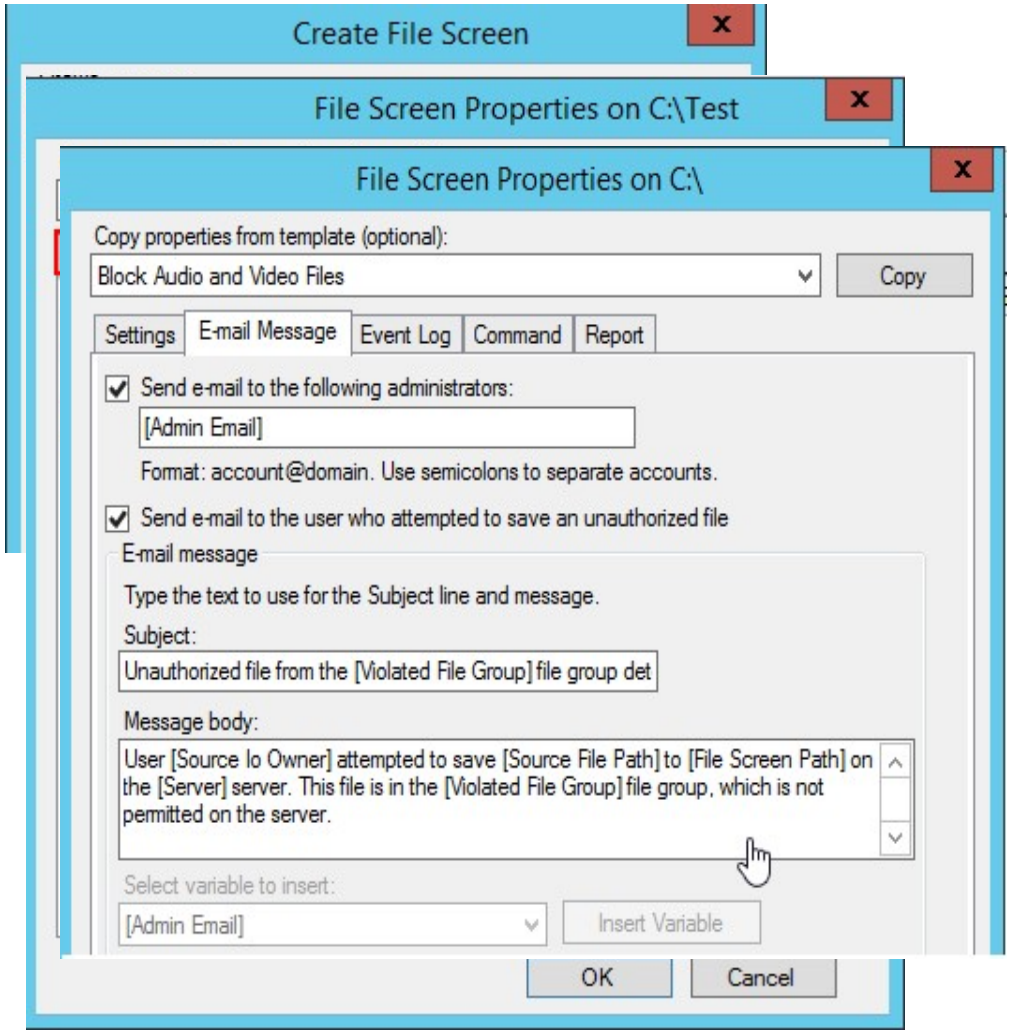
- Recovery to known Good Dataset, RRPO (Ransomware Recovery Point Objective)

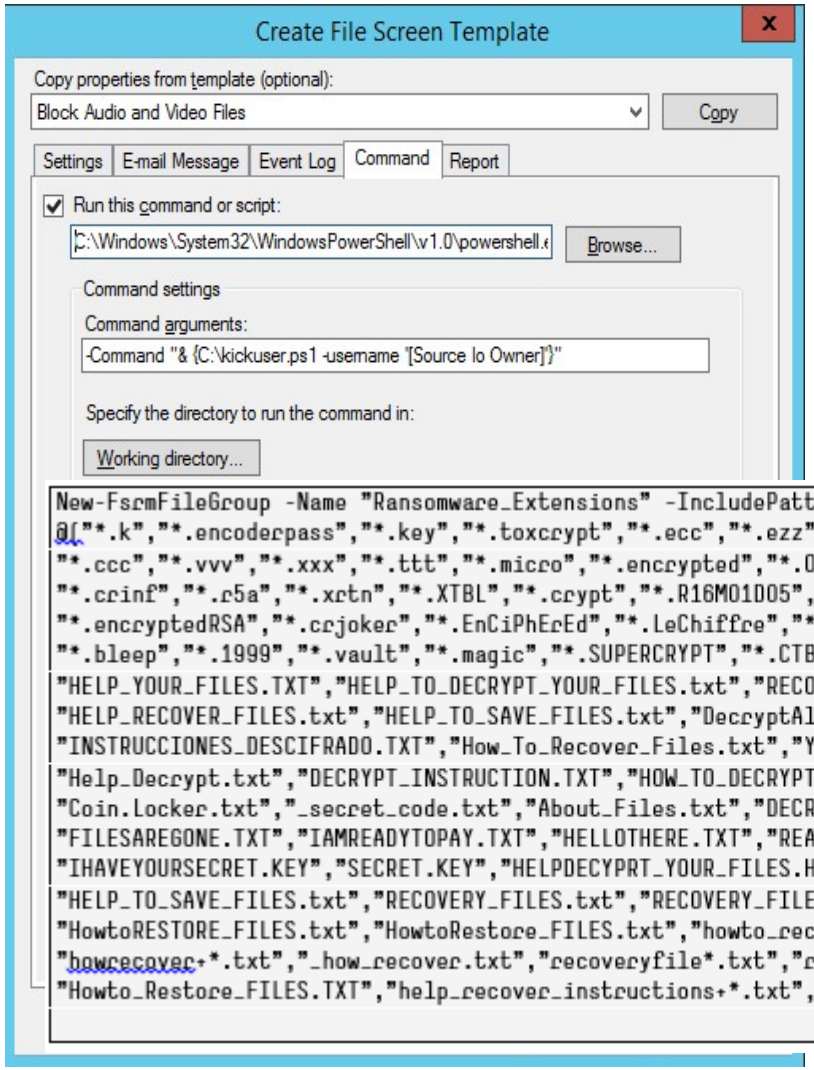
Harden your Servers and Infrastructure

- Nothing in this presentation eliminates (or lessens) you need for existing controls and hardening;
  - Continue to implement RBAC and Least-Privilege Access
  - Continue to implement IDS, Firewalls, ACLs, AAA, etc.
  - Ensure that Clients and Servers are accepting all security updates/patches
  - Eliminate older Client and Server OS Support, natively less secure
  - Ensure that Anti-virus and Malware detection is up to date
  - Implement Audits and File Screens where possible
- Follow NIST recommendations & CISSP best practices

  https://www.nist.gov/system/files/documents/2021/01/13/Getting-Started-NIST-Privacy-Framework-Guide.pdf

Example of how to setup a File Screen






```
New-FsrmFileGroup -Name "Ransomware_Extensions" -IncludePattern
@("*.k","*.encoderpass","*.key","*.toxcrypt","*.ecc","*.ezz","*.exx","*.zzz","*.xyz","*.aaa","*.abc",
"*.ccc","*.vvv","*.xxx","*.ttt","*.micro","*.encrypted","*.OMG!","*.locked","*.crypto","_crypt",
"*.crinf","*.r5a","*.xrtn","*.XTBL","*.crypt","*.R16M01D05","*.pzdc","*.good","*.LOL!","*.RDM","*.HA3"
"*.encryptedRSA","*.crjoker","*.EnCiPhErEd","*.LeChiffre","*.keybtc@inbox_com","*.0x0","*.RRK",
"*.bleep","*.1999","*.vault","*.magic","*.SUPERCRYPT","*.CTBL","*.CTB2","*.locky","HELPDECRYPT.TXT",
"HELP_YOUR_FILES.TXT","HELP_TO_DECRYPT_YOUR_FILES.txt","RECOVERY_KEY.txt","HELP_RESTORE_FILES.txt",
"HELP_RECOVER_FILES.txt","HELP_TO_SAVE_FILES.txt","DecryptAllFiles.txt","DECRYPT_INSTRUCTIONS.TXT",
"INSTRUCCIONES_DESCIFRADO.TXT","How_To_Recover_Files.txt","YOUR_FILES.HTML","YOUR_FILES.url",
"Help_Decrypt.txt","DECRYPT_INSTRUCTION.TXT","HOW_TO_DECRYPT_FILES.TXT","ReadDecryptFilesHere.txt",
"Coin.Locker.txt","_secret_code.txt","About_Files.txt","DECRYPT_ReadMe.TXT","DecryptAllFiles.txt",
"FILESAREGONE.TXT","IAMREADYTOPAY.TXT","HELLOTHERE.TXT","READTHISNOW!!!.TXT","SECRETIDHERE.KEY",
"IHAVEYOURSECRET.KEY","SECRET.KEY","HELPDECYPRT_YOUR_FILES.HTML","help_decrypt_your_files.html",
"HELP_TO_SAVE_FILES.txt","RECOVERY_FILES.txt","RECOVERY_FILE.TXT","RECOVERY_FILE*.txt",
"HowtoRESTORE_FILES.txt","HowtoRestore_FILES.txt","howto_recover_file.txt","restorefiles.txt",
"howrecover+*.txt","_how_recover.txt","recoveryfile*.txt","recoverfile*.txt","recoveryfile*.txt",
"Howto_Restore_FILES.TXT","help_recover_instructions+*.txt","_locky_recover_instructions.txt"]
```


Start Ongoing Monitoring

- Monitoring should include the following metrics
  - File System Free Space – Data Set Growth Rate
  - Compression & Deduplication & Thin Provisioning Rate
  - Read/Write Ratio
  - Performance (IO/s & MB/s)
  - Array Based Snapshot Size
- Baseline and Monitoring Metrics specifics
  - Should have granularity of hourly for each counter
  - Should have a history of up to a year or more

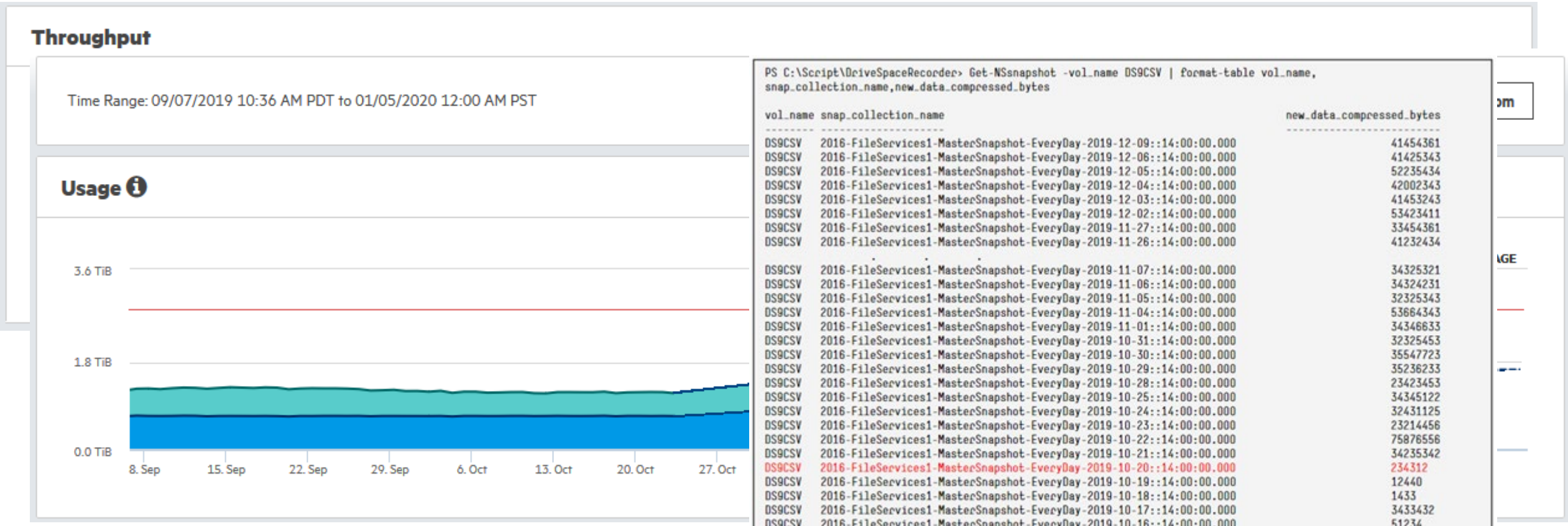
What Constitutes an Anomaly

- The following are all symptoms of an infection
  - The Ratio of Read/Write will shift dramatically towards 50:50%
  - The File System Free Space will not change to match the significant increase in write traffic (indicating massive overwrites instead of new files)
  - The Compression/Deduplication rate of the new data will dramatically approach 0% savings
  - The Performance of the file system will increase significantly, and regular patterns which include ‘quieter’ times will be lost.
- Common additional Actions of Ransomware
  - Disables VSS (Volume Shadow Services) based Snapshots and deletes existing snapshots
  - Disables classic backup software (agents) that lives on host.
  - Disables local auditing or metrics when possible.
  - Ransomware commonly drops instruction files for the victim on the file system as well.

Isolate and Determine start of infection

- This deck and presentation is far too short to discuss the process used to cleanse the infected machine.
  - This may include a fresh OS installation, resetting many Domain Credentials, disabling local accounts and investigating other machines in periphery also infected.
  - BUT….. You can easily disconnect the Data Volumes from an infected machine, and revert them back to the most recent backup before the infection encrypted the dataset.
  - You will need granular long-lived snapshots. Using the size of these snapshots can also help determine the start-of-infection date to guide your restoration.

Examples of these metrics




```
PS C:\Script\DriveSpaceRecorder> Get-NSsnapshot -vol_name DS9CSV | format-table vol_name,
snap_collection_name,new_data_compressed_bytes

vol_name snap_collection_name                                                    new_data_compressed_bytes
-------- -------------------                                                     -------------------------
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-09::14:00:00.000                      41454361
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-06::14:00:00.000                      41425343
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-05::14:00:00.000                      52235434
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-04::14:00:00.000                      42002343
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-03::14:00:00.000                      41453243
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-12-02::14:00:00.000                      53423411
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-27::14:00:00.000                      33454361
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-26::14:00:00.000                      41232434
                  .       .       .
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-07::14:00:00.000                      34325321
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-06::14:00:00.000                      34324231
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-05::14:00:00.000                      32325343
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-04::14:00:00.000                      53664343
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-11-01::14:00:00.000                      34346633
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-31::14:00:00.000                      32325453
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-30::14:00:00.000                      35547723
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-29::14:00:00.000                      35236233
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-28::14:00:00.000                      23423453
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-25::14:00:00.000                      34345122
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-24::14:00:00.000                      32431125
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-23::14:00:00.000                      23214456
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-22::14:00:00.000                      75876556
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-21::14:00:00.000                      34235342
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-20::14:00:00.000                        234312
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-19::14:00:00.000                         12440
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-18::14:00:00.000                          1433
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-17::14:00:00.000                       3433432
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-16::14:00:00.000                         51234
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-15::14:00:00.000                          1212
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-14::14:00:00.000                         12123
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-13::14:00:00.000                      34564564
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-12::14:00:00.000                           342
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-11::14:00:00.000                         32141
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-10::14:00:00.000                          3414
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-09::14:00:00.000                         34352
DS9CSV   2016-FileServices1-MasterSnapshot-EveryDay-2019-10-08::14:00:00.000                         30232
```


Where and How this works

- This Method works without the need for the Storage Device to crack and monitor the file system directly.
  - This means it works for File Services, and works on locked or unavailable files,
  - It also works for Virtual Machines hosted on VHDs, VMDKs, VMFS

- This Method however does not work in two very specific use cases
  - When data is written from the host pre-encrypted such as using host based full disk encryption such as Bit-locker
    - The benefits of Thin Provisioning, Compression, and Deduplication are also lost.
    - For At-Rest Encryption, the storage device itself should provide this functionality
  - When the dataset to be protected already mimics the near-zero compression or deduplication rate, and the workload already matches the target 50:50 read/write ratio

Vendor Considerations : Customer Benefits

- Phone Home Type Support should include performance Metrics
  - Should include a historic perspective and modeling
- Array should support space savings features; Thin, Compress, Dedupe
  - These should default on, and effects should be included in metrics
- Array Should support snapshots that are both granular & long life,
  - Expectation; minimum daily snapshots, and lifetime should exceed 3-6 months
- Array should support at-rest encryption;
  - Cant fault OS for host-based at-rest encryption if you don't offer same protection

Please take a moment to rate this session.

Your feedback is important to us.

