SYNACKTIV

Bypassing EDRs
SentinelOne agent analysis

Matthieu Barjole

x33fcon 2025

Context

- **Quick / dirty SentinelOne agent analysis**
  - Configuration storage
  - Access control
  - Communication with console
- **Windows-focused**

Configuration storage

SYNACKTIV

- **Two configuration folders**

```
$ ls -l 'Program Files/SentinelOne/Sentinel Agent 24.1.5.277/config'
AgentUid.json
LocalConfig.json
UserConfig.json
[...]

$ ls -l ProgramData/Sentinel/assets
14078386573983218 89.asset
14078386576132123 62.asset
14078386581222398 99.asset
[...]
assets
```

- **Encrypted data** for most of them

```
$ cat config/UserConfig.json
{"mgmtServer":"https://hello-123.sentinelone.net","newConfiguration":false,"proxy":"","site":"0123456789abcdef"}

$ xxd config/AgentUid.json
00000000: 0bf5 caed ef7f 4e13 dd68 67af 74f6 c794  ......N..hg.t…
```

Configuration storage

SYNACKTIV

- **Encryption analysis**
  - Content is similar, common prefix + on in two byte is the same + it's UTF-16 JSON

```
$ xxd AgentUid.json | head -1
00000000: 0bf5 caed ef7f 4e13 dd68 67af 74f6 c794  ......N..hg.t...

$ xxd Policy.json | head -1
00000000: 0bf5 caed ef7f 4e13 e368 75af 78f6 cd94  ......N..hu.x...

$ xxd UserConfig.json | head -1
00000000: fffe 7b00 2200 6d00 6700 6d00 7400 5300  ..{.".m.g.m.t.S.
```

  - **XOR** with a **hardcoded key** :)
  - **Exclusions decryption**

```
$ python3 decrypt.py 14078386622713298 49.asset
[{ "pathSpec": "C:\Windows\Program Files\App\",
   "scope": "subfolders", [...] }]
```

Configuration storage

SYNACKTIV

- **Access control**
  - Before Nov. 2024, both folders accessible to all users!
  - Since Oct. 30, `assets` is restricted to admins, but `config` still available

```
PS C:\Program Files\SentinelOne\Sentinel Agent 24.1.5.277\config> icacls Policy.json
BUILTIN\Administrators:(I)(RX)
BUILTIN\Users:(I)(RX)
[...]

PS C:\ProgramData\Sentinel\assets> icacls assets
BUILTIN\Administrators:(OI)(CI)(RX)
[...]
```

  - But we lost access to `assets` with exclusions :(

Communication

Authentication

SYNACKTIV

- **Agent UUID** generated on registration
  - Used as authentication token, stored in `config/AgentUID.json`
  - But `config` folder accessible to **all users**!

```
PS C:\Program Files\SentinelOne\Sentinel Agent 24.1.5.277\config> icacls AgentUID.json
BUILTIN\Users:(I)(RX)

$ python3 decrypt.py config/AgentUID.json
{"_uid":"0123456789abcdef0123456789abcdef",[...]}
```

  - New access to exclusions **exclusions** :)

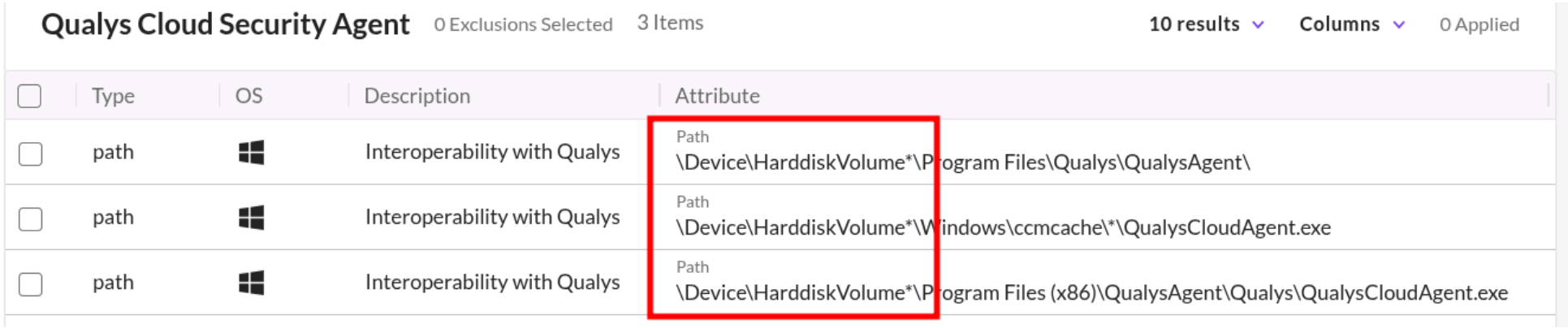
```
$ curl https://hello-123.sentinelone.net/api/v1.6/assets/1234567891234567890 \
  -H 'x-uuid: 0123456789abcdef0123456789abcdef'
  [{ "pathSpec": "C:\Windows\Program Files\App\",
     "scope": "subfolders", [...] }]
```

Exclusions

Dangerous patterns

SYNACKTIV

- **Exclusion templates offered by SentinelOne**



Qualys Cloud Security Agent 0 Exclusions Selected 3 Items 10 results Columns 0 Applied

Type	OS	Description	Attribute
path		Interoperability with Qualys	Path \Device\HarddiskVolume*\Program Files\Qualys\QualysAgent\
path		Interoperability with Qualys	Path \Device\HarddiskVolume*\Windows\ccmcache*\QualysCloudAgent.exe
path		Interoperability with Qualys	Path \Device\HarddiskVolume*\Program Files (x86)\QualysAgent\Qualys\QualysCloudAgent.exe

- `\Device\HarddiskVolume*` disk-agnostic syntax, but `*` also matches `\` :)

> If a wildcard is used with harddiskvolume, you may exclude more devices than you intended.
> **Example**: You want to exclude `\Device\HarddiskVolume0\Test\` you create this exclusion:
> `\Device\HarddiskVolume*\Test\.`
>
> Now these paths are also excluded because of the wildcard:
>
> `\Device\HarddiskVolume8\software\test\`
> `\Device\HarddiskVolume12\engineering\study\test\`

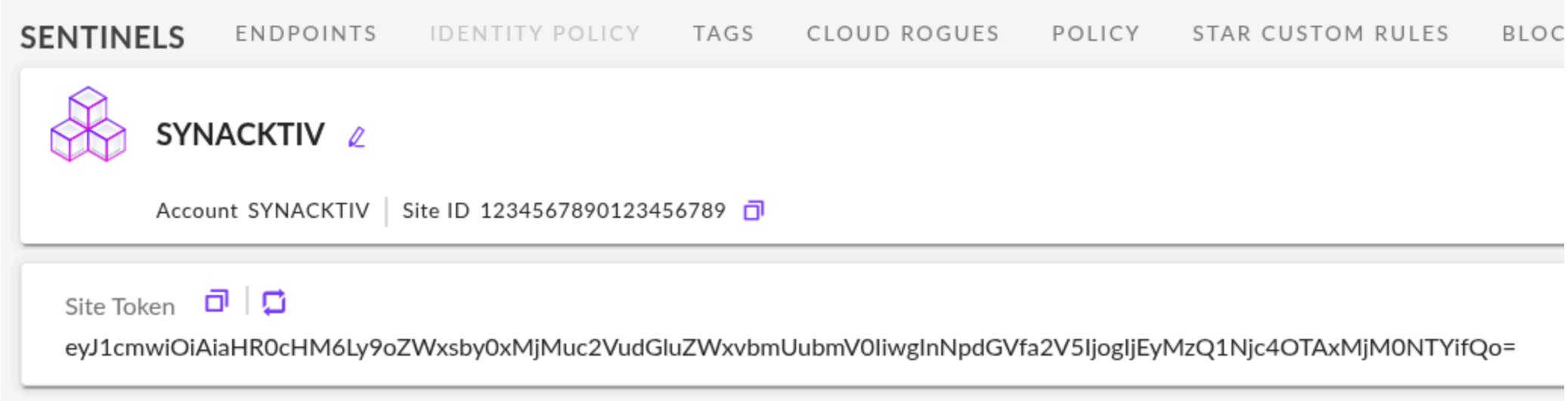
- Create `C:\Users\user\AppData\Program Files\Qualys\QualysAgent\safe.exe`

Agent registration

Token

SYNACKTIV

- Token specific to **site** or **group** to register a new agent




```
{"url": "https://hello-123.sentinelone.net", "site_key": "0123456789abcdef"}   # Site
{"url": "https://hello-123.sentinelone.net", "site_key": "g_0123456789abcdef"} # Group
```

- But it is removed from the endpoint after registration, right?

Agent registration

Token

SYNACKTIV

- `site_key` preserved after agent registration, **exposed on all endpoints**!
  - Accessible to all users again, not even encrypted

```
PS C:\Program Files\SentinelOne\Sentinel Agent 24.1.5.277\config> icacls UserConfig.json
BUILTIN\Users:(I)(RX)

$ cat config/UserConfig.json
{"mgmtServer":"https://hello-123.sentinelone.net","newConfiguration":false,"proxy":"","site":"0123456789abcdef"}
```

- **Opportunities**
  - Registering new agents to trigger fake alerts → decoy
  - Read configuration from the console → exclusions
  - `site_key` cannot be revoked → must migrate all agents to new site / group

Detection

Blue side

SYNACKTIV

- **What about detection?**
  - No telemetry on file reads :(
  - Cannot detect access to configuration
  - Specific event log for agent registration but rarely integrated in detections

Conclusion

SYNACKTIV

- **Recommendations**
  - Define exclusions from **hash or signature**
  - **Limit** exclusion scope to specific group, not site
  - **Avoid** using `*` in path exclusions, do not use SentinelOne-provided templates
  - **Audit** EDRs as any other software

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://bsky.app/profile/synacktiv.com

https://synacktiv.com