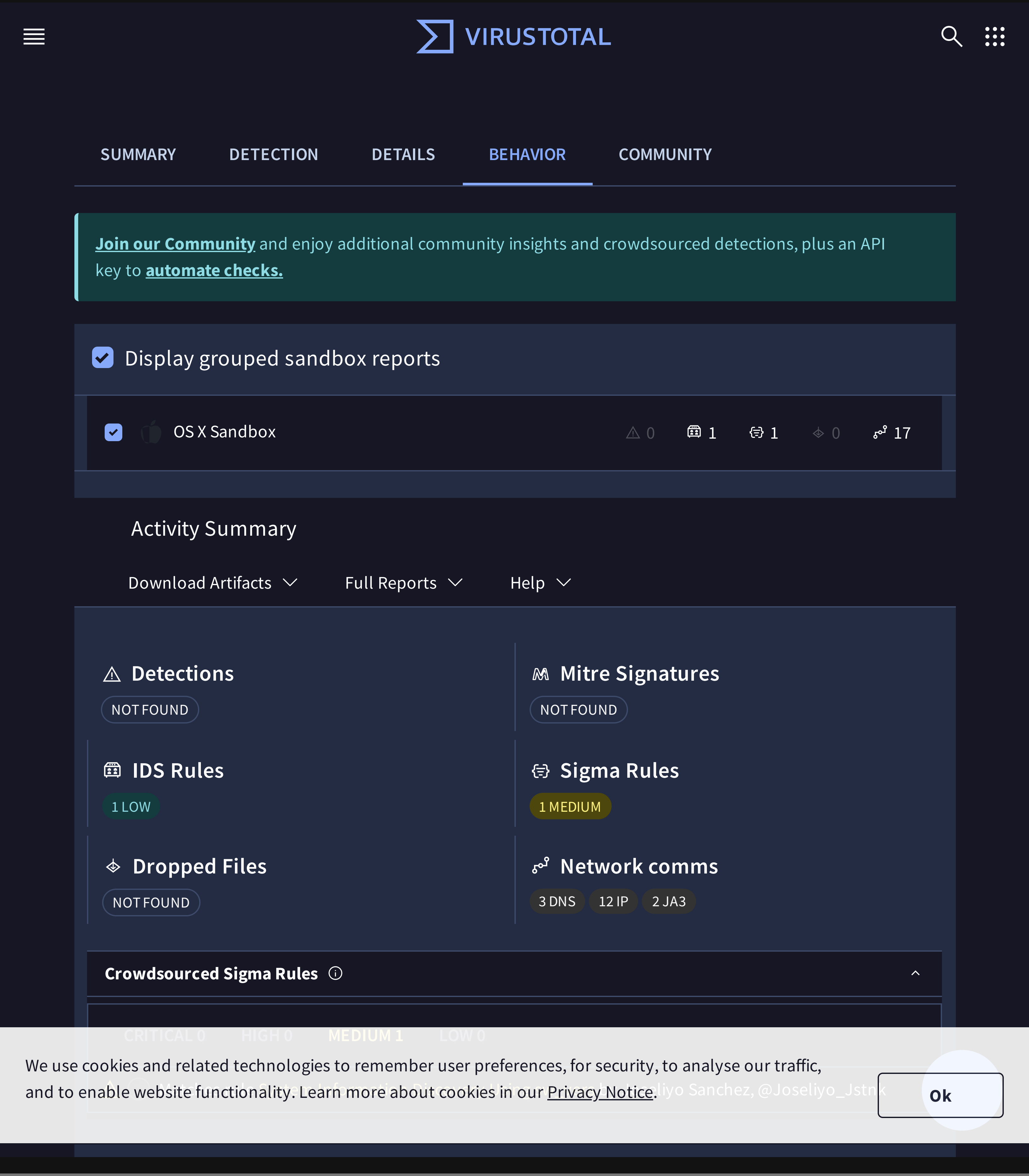


SUMMARY DETECTION DETAILS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

☑ Display grouped sandbox reports

☑ OS X Sandbox ⚠ 0 1 1 0 17

Activity Summary

Download Artifacts ⌄ Full Reports ⌄ Help ⌄

⚠ **Detections**

NOT FOUND

Mitre Signatures

NOT FOUND

IDS Rules

1 LOW

Sigma Rules

1 MEDIUM

Dropped Files

NOT FOUND

Network comms

3 DNS 12 IP 2 JA3

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.

Ok

Crowdsourced IDS rules

⚠ Matches rule (tcp) experimental TCP options found

Network Communication

DNS Resolutions

- mask-api.fe.apple-dns.net
- security.hashkeytech.pro
- security.hashkeytech.pro.local

IP Traffic

- TCP 104.73.28.93:443
- TCP 184.31.52.187:443
- TCP 17.248.195.69:443
- TCP 17.253.7.202:443
- TCP 23.46.248.19:443
- TCP 172.64.149.23:80
- TCP 23.203.100.142:443
- TCP 172.66.43.196:443
- TCP 104.18.13.252:443
- TCP 17.253.21.208:443

JA3 Digests

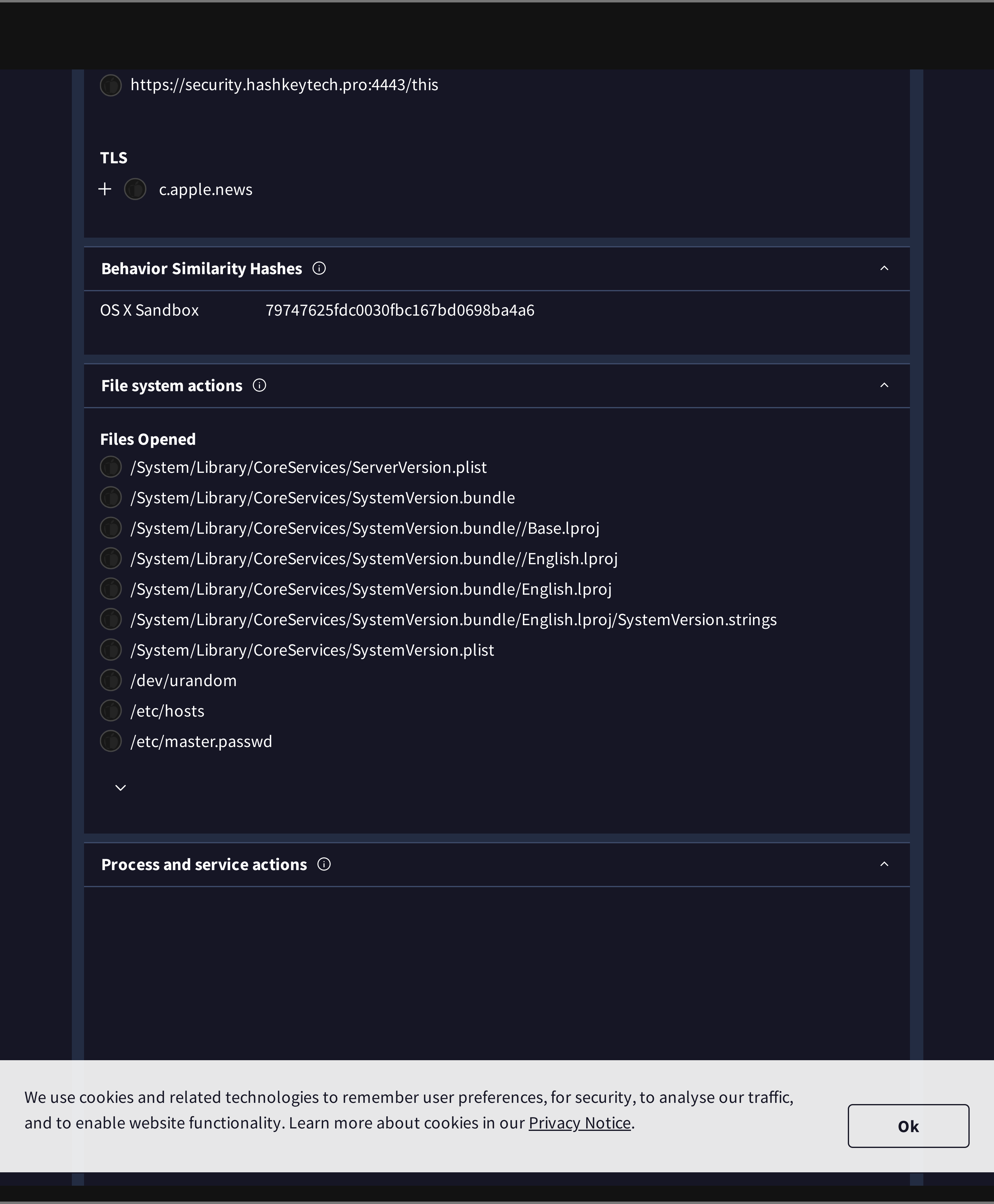
- 773906b0efdefa24a7f2b8eb6985bf37
- fb3660676bafc9799c86bd51a1ea12f5

Memory Pattern Domains

- hw.ncpuinvalidlookup
- security.hashkeytech.pro:444

Memory Pattern Urls

- http://hw.ncpuinvalidlookup
- https://security.hashkeytech.pro:4443/
- https://security.hashkeytech.pro:4443/N4215/adj/amzn.us.sr.aps



https://security.hashkeytech.pro:4443/this

TLS

+ c.apple.news

Behavior Similarity Hashes

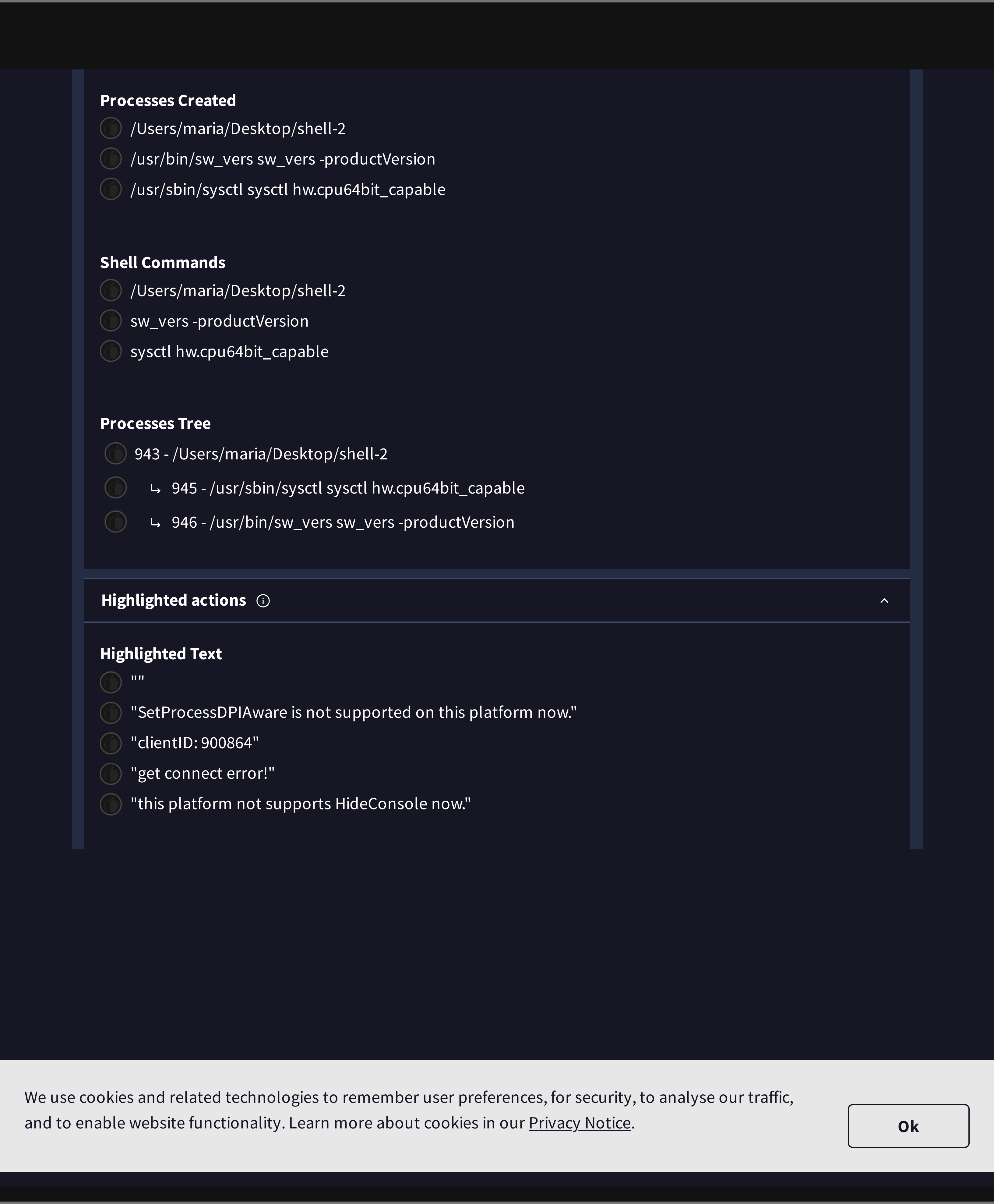
OS X Sandbox	79747625fdc0030fbc167bd0698ba4a6

File system actions

Files Opened

- /System/Library/CoreServices/ServerVersion.plist
- /System/Library/CoreServices/SystemVersion.bundle
- /System/Library/CoreServices/SystemVersion.bundle//Base.lproj
- /System/Library/CoreServices/SystemVersion.bundle//English.lproj
- /System/Library/CoreServices/SystemVersion.bundle/English.lproj
- /System/Library/CoreServices/SystemVersion.bundle/English.lproj/SystemVersion.strings
- /System/Library/CoreServices/SystemVersion.plist
- /dev/urandom
- /etc/hosts
- /etc/master.passwd

Process and service actions



Processes Created

- /Users/maria/Desktop/shell-2
- /usr/bin/sw_vers sw_vers -productVersion
- /usr/sbin/sysctl sysctl hw.cpu64bit_capable

Shell Commands

- /Users/maria/Desktop/shell-2
- sw_vers -productVersion
- sysctl hw.cpu64bit_capable

Processes Tree

```
943 - /Users/maria/Desktop/shell-2
    ↳ 945 - /usr/sbin/sysctl sysctl hw.cpu64bit_capable
    ↳ 946 - /usr/bin/sw_vers sw_vers -productVersion
```

Highlighted actions ⓘ

Highlighted Text

- ""
- "SetProcessDPIAware is not supported on this platform now."
- "clientID: 900864"
- "get connect error!"
- "this platform not supports HideConsole now."