

CryptoSpike

ProLion

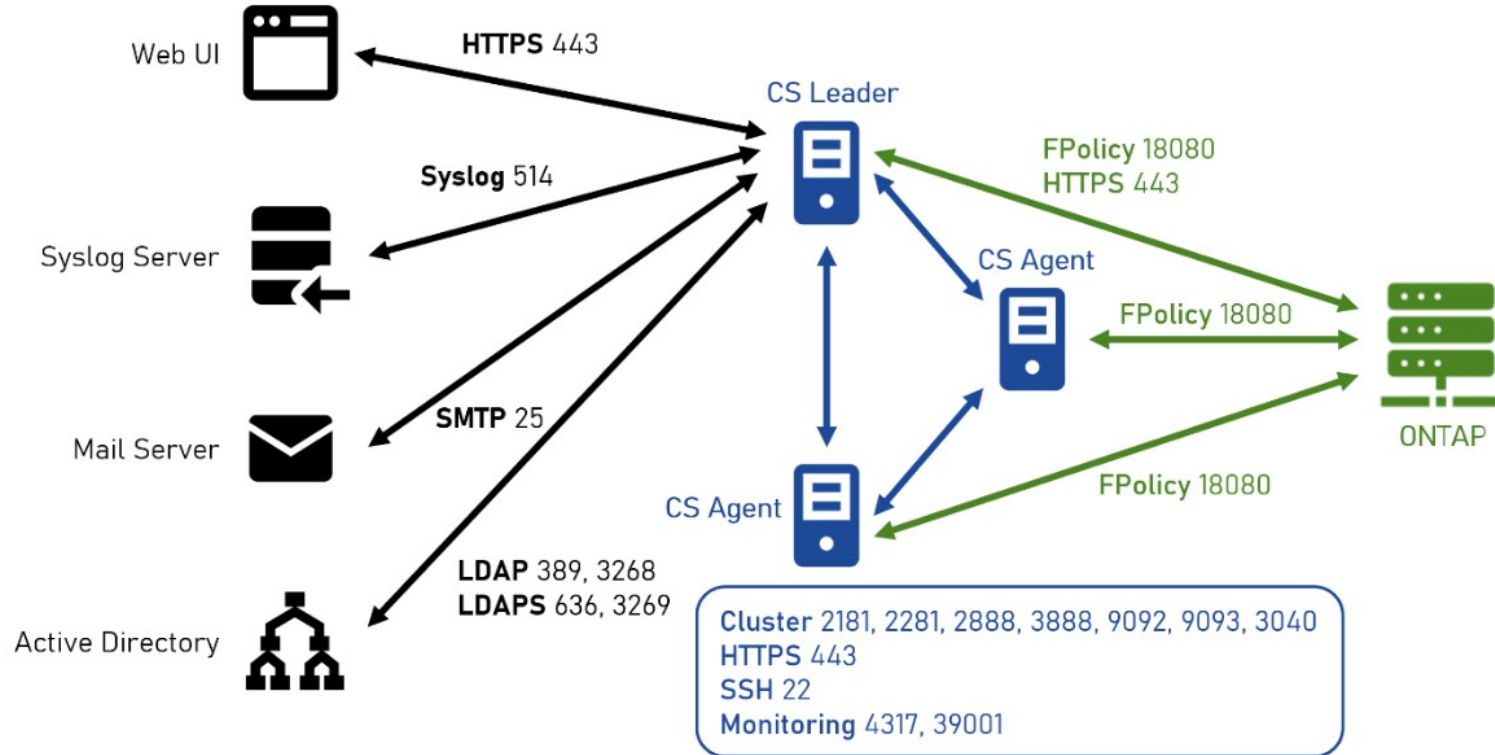
Protection contre les ransomwares

S P É C I F I C A T I O N S I M F T

- Protection stockage NetApp ONTAP
- Machine virtuelle
 - 8 cœurs
 - 24 Go de ram
 - 50 Go / 100 Go / 300 Go
- Alpine Linux 3.15
- Conteneurs
- Compte ldap AD
- Mode apprentissage / actif
- Blocage
 - extensions
 - comportements
- Restauration
- Accompagnement : Sébastien SOKOLOFF

ARCHITECTURE

ONTAP Environments



** and any other port that may be specific to your environment for running SYSLOG, MAIL, AD, etc...*

DASHBOARD

ProLion CryptoSpike sysadm

- Dashboard
- Audited Users
- File Activity
- Landscape
- Rules
- User Management
- Settings
- System

Latest Blockings

| Block Time | Name / ID | Block rule | First block file |
|---------------------|-----------|---------------|--|
| 2023-09-20 16:58:41 | 53333 | stub | /mnt/Work/03-July2021_Events/zz-JSC_20230920/Belleflamme/tsmp_tools/external/pfread_var.stub |
| 2023-09-05 16:46:38 | 43832 | lion | /mnt/Work/09-2023/Spotlight-V100/Store-V2/2547497D-99DD-43D8-9B4B-8A5B24899F83/tmp.Lion |
| 2023-10-06 16:50:42 | 25604 | done | /mnt/conda/pkgs/mysql-5.7.24-h721c034_2/mysql-test/collections/default.release.done |
| 2023-09-05 10:05:43 | 53456 | replaceRule | /mnt/vim/pack/kite/start/vim-plugin/LICENSE |
| 2023-10-02 11:48:54 | 53456 | overWriteRule | /mnt/zotero/zotero/uwv4lqe.default/cookies.sqlite-shm |
| 2023-09-11 14:25:26 | 53456 | random | /mnt/GITLAB/AVBP_AVTP_712_RADIIATIVE_working/avbp-7.12.0/LIBRARIES/Zoltan_v3.83/test/hg_simple/zdrive.inp.phg.random |
| 2023-09-04 09:17:46 | 43832 | read.txt | /mnt/Documents/ARCH/dokuwiki/inc/lang/id/read.txt |
| 2023-09-04 15:02:29 | 53456 | warning.txt | /mnt/Téléchargements/alpha100/AVTP01/WARNING.TXT |
| 2023-09-12 11:23:14 | 31308 | missina | /mnt/cache/JetBrains/PyCharmCE2023.2/python_stubs/cache/ |

Items per page: 10 1 - 10 of 15

Status Overview

Cluster: VENOM SVM's

IOPS

Hour 24 Hours 7 Days 14 Days

File Events/s

0

09:10 09:20 09:30 09:40 09:50 10:00

Legend: Total Analyzed User Events Ignored/Blocked User Events

Block count

Hour 24 Hours 7 Days 14 Days

15

Users

17

13

09:30 10:00

Legend: Blocked users

CryptoSpike v3.1.4 ©2024 ProLion GmbH

UTILISATEURS BLOQUES

ProLion
CryptoSpike
sysadm

- Dashboard
- Audited Users
- Users
- Incidents
- File Activity
- Landscape
- Rules
- User Management
- Settings
- System

Blocked only



Unblock all
Resolve users
Refresh

Showing 15 users (filtered from 222 total)


| <input type="checkbox"/> | Blocked | Name | ID | First block file | Block rule | Block summary | Last block | |
|--------------------------|------------------------------------|-----------------|----------------------|--|---------------|---------------|---------------------|--|
| <input type="checkbox"/> | - | unresolved user | 53333 | /home/.../Work/03-July2021_Events/zz-JSC_20230920/Belleflamme/tsmp_tools/external/pfread_var.stub | stub | | 2023-09-20 16:58:41 | |
| <input type="checkbox"/> | - | unresolved user | S-1-5-21-29092818... | /home/.../cle usb luca 09-2023/.Spotlight-V100/Store-V2/2547497D-99DD-43D8-9B4B-8A5B24899F83/tmp.Lion | lion | | 2023-09-05 16:46:38 | |
| <input type="checkbox"/> | - | unresolved user | 25604 | /home/.../conda/pkgs/mysql-5.7.24-h721c034_2/mysql-test/collections/default.release.done | done | | 2023-10-06 16:50:42 | |
| <input type="checkbox"/> | - | unresolved user | 48371 | /home/.../vim/pack/kite/start/vim-plugin/LICENSE | replaceRule | | 2023-09-05 10:05:43 | |
| <input type="checkbox"/> | - | unresolved user | 51293 | /home/.../zotero/zotero/uwv4lqe.default/cookies.sqlite-shm | overWriteRule | | 2023-10-02 11:48:54 | |
| <input type="checkbox"/> | - | unresolved user | 53286 | /home/.../GITLAB/AVBP_AVTP_712_RADIATIVE_working/avbp-7.12.0/LIBRARIES/Zoltan_v3.83/test/hg_simple/zdrive.inp.phg.random | random | | 2023-09-11 14:25:26 | |
| <input type="checkbox"/> | - | unresolved user | 43832 | /home/.../Documents/ARCH/dokuwiki/inc/lang/id/read.txt | read.txt | | 2023-09-04 09:17:46 | |
| <input type="checkbox"/> | - | unresolved user | 53456 | /home/.../Téléchargements/alpha100/AVTP01/WARNING.TXT | warning.txt | | 2023-09-04 15:02:29 | |
| <input type="checkbox"/> | - | unresolved user | 31308 | /home/.../.cache/JetBrains/PyCharmCE2023.2/python_stubs/cache/d62206c38b781a05c4b2bcb04e0c9eaca0954f14ed995a378ff7494a8a38d7fc.fai missing led_pandas_libs.missing | | | 2023-09-12 11:23:14 | |
| <input type="checkbox"/> | - | unresolved user | 55554 | /home/.../.cache/JetBrains/PyCharmCE2021.1/python_stubs/cache/abe174beddeef76dd7887231aa8bc3f9539df25c1c04bd9aae0d7cd9735addbc/fa missing iled_pandas_libs.missing | | | 2023-10-10 10:39:51 | |
| <input type="checkbox"/> | - | unresolved user | 47097 | /home/.../vscode/extensions/.7201b83c-d9fd-4521-819a-78edb8dbe59f/omnisharptest/omnisharpIntegrationTests/testAssets/BasicRazorApp2_1/Pages/razor>ErrorHaver.razor | | | 2023-09-04 14:30:05 | |
| <input type="checkbox"/> | - | unresolved user | 26214 | /home/.../local/share/okular/docdata/9670146.escalademag_12.pdf.xml | *.ESCAL* | | 2023-09-29 17:21:58 | |
| <input type="checkbox"/> | - | unresolved user | 37745 | /home/.../conda/pkgs/mysql-5.7.24-h721c034_2/mysql-test/collections/default.release.done | done | | 2023-09-26 11:25:32 | |

Items per page: 500
1 - 15 of 15



RÈGLES DE BLOCCAGE

 **CryptoSpike** sysadm 

- Dashboard
- Audited Users >
- File Activity
- Landscape >
- Rules**
- User Management >
- Settings >
- System >



CryptoSpike v3.1.4
©2024 ProLion GmbH 

File event blacklist

| Config Id | Name | Description | Published At | Actions |
|-----------|-------------------|-----------------------------------|--------------|---|
| 2152 | Prolion blacklist | The prolion application blacklist | - |   |



[+ Add Configuration](#)

File event ignored users

| Config Id | Name | Description | Published At | Actions |
|-----------|-----------------------|---------------------------------------|---------------------|---|
| 2155 | Prolion ignored users | The prolion application ignored users | 2023-02-16 12:23:56 |   |



[+ Add Configuration](#)

Analyzer file operation patterns

| Config Id | Name | Description | Published At | Actions |
|-----------|------------------------------------|---|---------------------|---|
| 2153 | Prolion file operation pattern ... | The prolion application file operation patterns | 2023-06-28 10:00:58 |   |

[+ Add Configuration](#)

Analyzer blacklist hits

| Config Id | Name | Description | Published At | Actions |
|-----------|-------------------------------|---|---------------------|---|
| 2154 | Prolion blacklist hit counter | The prolion application blacklist hit counter | 2023-04-17 11:07:52 |   |

[+ Add Configuration](#)