www.synapsa.tech SYNAPSA

SYNAPSA
Cyber Security Automation

CYBER SECURITY AUTOMATION

Out-of-the-box **automation powered platform** that allows significant ITOps and SecOps time savings and ensures the disclosure of security gaps within minute.

FTE SAVINGS

Significant workforce savings within daily IT and Security Operation

FASTER RESPONSE

Speed up Incident Response and Threat Mitigation to reduce impact

AUTOMATION

Built-in intelligence simplifying Compliance Check, Threat and Incident Management

TODAY'S DAILY OPERATION CHALLENGES

LACK OF AUTOMATION

Not enough resources to asses all important events

INCIDENT RESPONSE DELAY

Long delay between threat detection and mitigation

CHANGE MANAGEMENT OVERLOADING

Manually solving tasks is highly time consuming

ABOUT SYNAPSA NETWORKS

Synapsa Networks is developing a Synapsa Platform with built-in intelligence focusing on Security Compliance Check and Automation to prevent human and technology failures, **save workforce and improve response time**.

The **Synapsa Platform** performs a continuous audit, control and enforcement over configuration and security policies rulesets, **allows IT tools to talk to each other** without alert fatigue, provides threat and data feeds management within a single pane of glass. That all just **simplifies and speeds up** daily operation to ensure business continuity in real time.

www.synapsa.tech

info@synapsa.tech

Identifying of security breach takes organizations 212 days and another 75 days to actually contain it.

Cybersecurity without automation is a losing game.

Synapsa Platform Benefits

Rapid time saving of daily operation

Significant workforce savings in daily Security, Network and IT operation

SecOps productivity acceleration

Time reduction in case of manual or automatic response on cybersecurity incidents

Overall workflow automation

Built-in intelligence simplifying Incident and Change management procedures

Current ecosystem integration

3rd party tools integrations to provide smooth automation

SYNAPSA PLATFORM

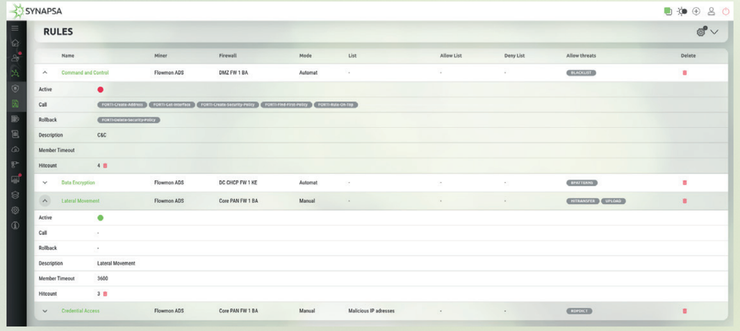
In the age of digital transformations, the increase in **cyber security threats**, alerts, daily operational tasks and the lack of resources, automation is one of the most effective options for ensuring critical **services availability** and **business continuity**.

It can be deployed literally anywhere and within a few minutes, we are leveraging **docker technology** to make you install based on your preferences. Typical **deployment takes less than 90 minutes** of your time, but saves hours of manual work.

INTERCONNECTOR

IT and Security Operation Automation

The middleware which **automatically processes input** data from any source (miner) capable of sending syslog such as SIEM, Firewalls, Proxy, Servers and other endpoints. By leveraging the built-in parsers it is possible to **extract any data and reuse** it in various automation tasks.

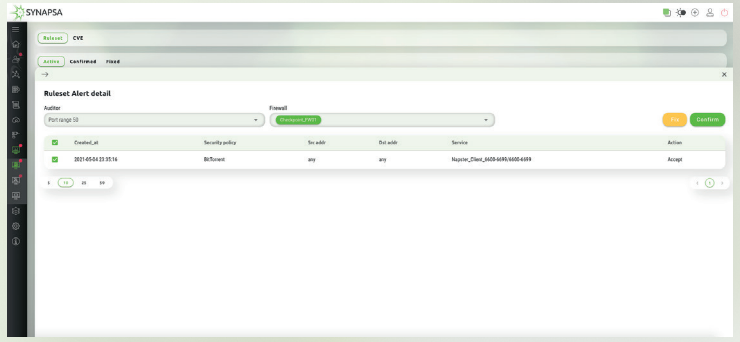


All the functionality is available **hassle free** from the GUI **without any scripting skills**. There is a built-in parser for any data coming from any source (miner). An action can be processed automatically or semi-automatically (requires human approval).

AUDITOR

Compliance Auditing and Integrity Check

Allows operators to have **complete control** over the configuration and compliance with any industry benchmark or standards making sure that there are no misconfigurations, dangerous rules, widely open policies or unavailability of critical services.

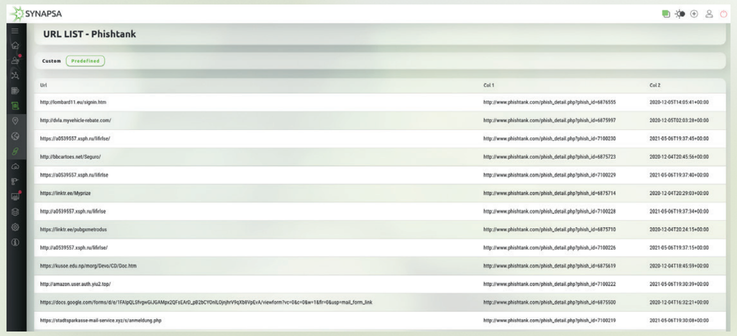


The “allow and forget” approach is not secure. There is a need to **constantly monitor the integrity** of the configuration and to make sure there is no hidden, forgotten or even purposely configured part, which could make you vulnerable.

DATA FEEDS

Intelligent External Dynamic Lists

Group of smart dynamic object lists consisting of **threat intelligence data** to feed your cybersecurity mitigation devices like firewalls, proxy or cloud infrastructure to **protect your environment** from the latest indicators of compromise (IoCs).

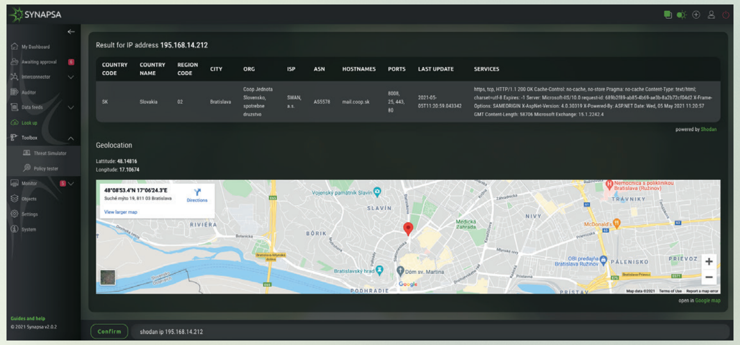


Intelligent IP, URL or DNS management, including automatic data removal in case a specific object is no longer being reported as malicious and brings the database query speed level to avoid API requests that are slow for high volume lookups in real-time.

LOOK UP

Threat Intelligence Enrichment

Single pane of glass for data enrichment from any 3rd party API provider, which allows analysts to easily fetch data and use it for event investigation.

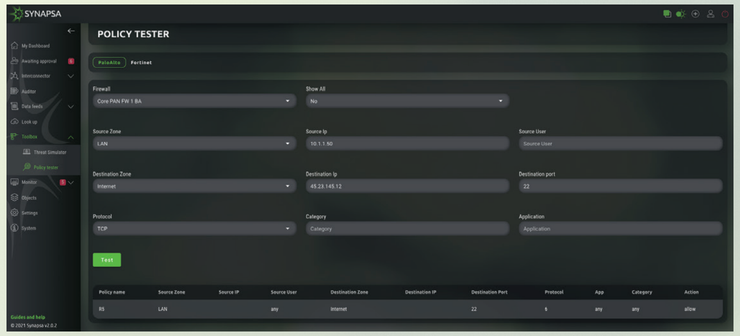


Offers war rooms to do analysis of a cyber security incident faster and allows the SOC team to cooperate in a single UI and provides faster **Mean Time to Response** (MTTR).

TOOLBOX

Threat and Policy Testing

User can provide a **simulation** of what will be the impact of a specific **threat** sent by a miner including all the actions as the threat is really reported.



Moreover user can **test** if a specific packet is allowed on the selected device's **ruleset** and which rule allows or denies the traffic. No need to touch the device, but the output is generated by a device's engine.

Synapsa Platform provides **full visibility** and complete overview of Compliance Status in the dashboard widgets aggregated for all the monitored devices, or individually for each asset to eliminate **over 90% of the time** spent on Audits. Moreover, it allows Continuous Monitoring and Automated Remediation to ensure assets are always in compliance within CIS or other industry benchmarks.

Speed-up mitigation time 10x within Cybersecurity Incident and Threat Management procedures thanks to **Synapsa Platform smooth deployment**, built-in integrations and parsers, custom rules and actions. **Improve data feeds management** and high speed data lookup techniques to decrease manual tasks with no alert fatigue and analyst burnout within the whole year 24/7.

Built-in integrations

paloalto NETWORKS, CHECK POINT, FORTINET, SOPHOS, Progress Flowmon, SURICATA, Office 365, aws, RIPE NCC RIPE NETWORK COORDINATION CENTRE, NIST, VIRUSTOTAL, BigData Cloud, PhishTank, ipstack, SHODAN, ipinfo.io, MA:CV:en:do:rs, host.io