synapsa_product sheet_v2-1_print.pdf 1 16.06.2021 16:48:07

www.synapsa.tech

SYNAPSA

SYNAPSA
Cyber Security Automation

CYBER SECURITY AUTOMATION

Save significant workforce in defensive security, incident and change management.
Automate, improve response time and manage workflow more efficiently.

FTE SAVINGS

Significant workforce savings in daily Security, Network and IT operation

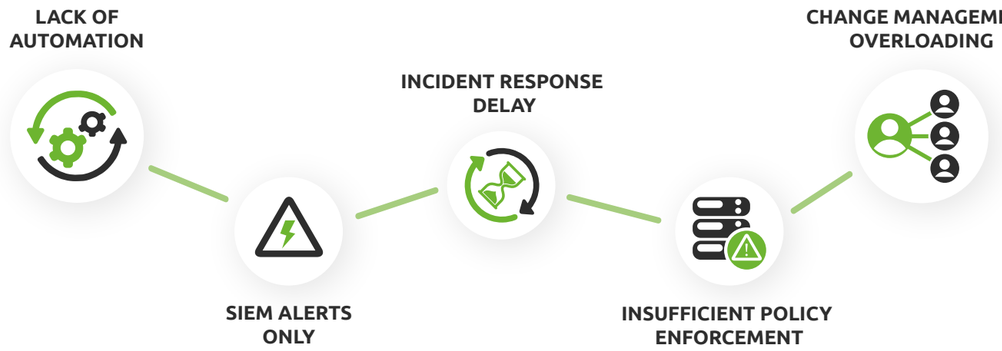
FASTER RESPONSE

Time reduction in case of manual or automatic response on cyber security incidents

AUTOMATION

Built-in intelligence simplifying Incident and Change management procedures

Today's daily operation challenges



ABOUT SYNAPSA NETWORKS

Synapsa Networks is developing a platform and **intelligent software tools** focusing on Incident and Change management procedures automation to prevent human and technology failures, save time and provide faster response.

The platform provides an environment that automatically interconnects devices and tools in IT infrastructure to **simplify and speed up the processes** in real time, to continue audit and control of policies setup and their enforcement and lastly, to **prevent human failures**.

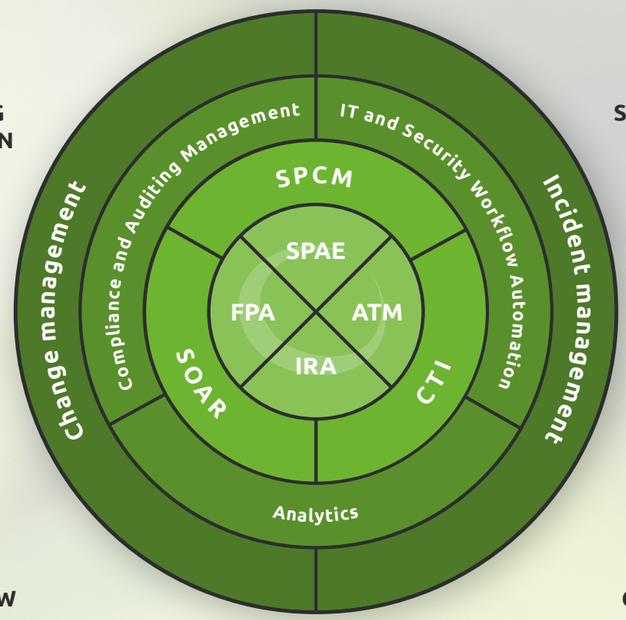
info@synapsa.tech

© Synapsa Networks

Synapsa platform provides easy to use application which helps to **save significant workforce** during Incident and Change management procedures.

RAPID TIME SAVING OF DAILY OPERATION

SECOPS PRODUCTIVITY ACCELERATION



OVERALL WORKFLOW AUTOMATION

CURRENT ECOSYSTEM INTEGRATION

synapsa_product sheet_v2-1_print.pdf 2 16.06.2021 16:48:11

SYNAPSA PLATFORM

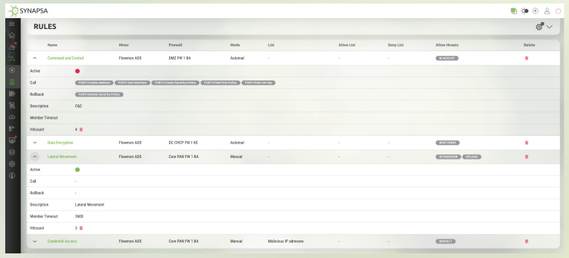
In the age of digital transformations, the increase in **cyber security threats**, alerts, daily operational tasks and the lack of sufficient resources, automation is one of the most effective options for ensuring critical **services availability** as well as **business continuity**.

The Synapsa platform provides an easy to use **docker powered secure API client** with access via a web user interface. Thanks to several pre-integrated modules, it is possible to automate the activities within Incident and Change management procedures.

INTERCONNECTOR

IT and SecOps Workflow Automation

Synapsa Interconnector provides intelligent API based interconnections between monitoring, security and change management tools to avoid time consuming manual procedures.

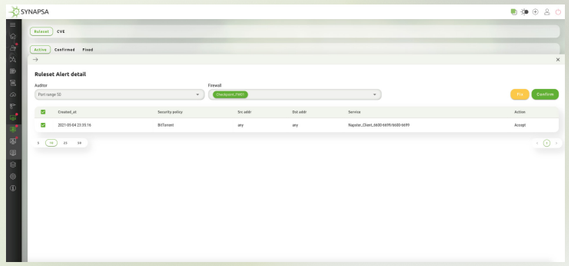


Thanks to predefined and custom parsers, it is able to **accelerate overall workflow activities** in daily operation. IT and SecOps Experts save time in the decision-making process and focus more on other necessary steps in daily operation.

AUDITOR

Compliance Auditing and Management

Prevention goes hand-in-hand with Detection and Response. **Synapsa Auditor** provides real-time API based Ruleset assessment on assets (e.g. Firewalls) to alert and avoid policy misconfigurations.

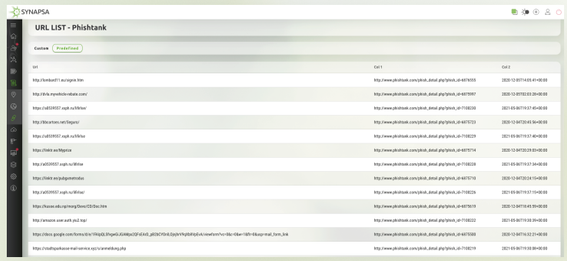


These policies might be a result of a human error or even of an intended malicious activity. It can detect, alert and **disable faulty policies** in **real time**.

DATA FEEDS

Constant Data Collection

Data collection combine first party data from internal sources with disparate data from other internal systems or third party data from external sources.

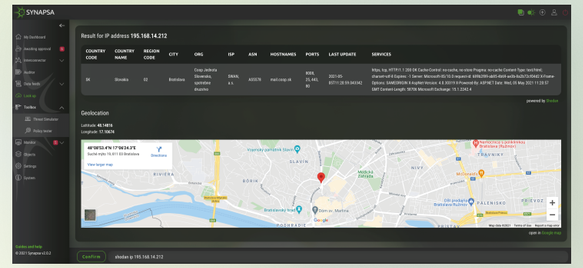


IP, URL or DNS Data Feeds make the data more useful by adding value to it regarding real time Incident Response Automation or Security Policy Enforcement.

LOOK UP

Cyber Threat Intelligence

Allows to **fetch information** about IP, Domain, URL, hash, threat and more useful details from 3rd party services and correlate it with internal telemetry into the incident log.

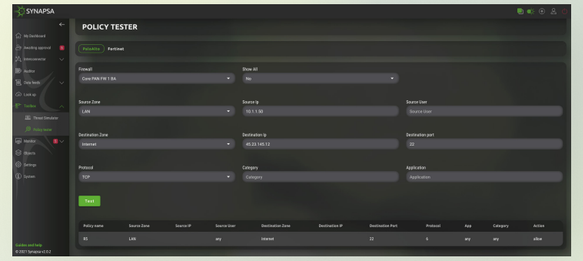


Operator can easily **analyse and enrich raw data** by a single click or command line without leaving Synapsa UI.

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.

In case of **Incident management** procedures IT and SecOps specialists need to be aware of all tasks, alerts, analyse all relevant events (often manually), check for false positives and decide the appropriate response or futher steps. It requires often **long term validation** and **approvals** through the **Change management** process. **Synapsa Platform** allows to use built-in integrations or to define, prepare, develop and deploy custom integrations for individual requirements and use cases covering.

It is ready for 3rd party tools integrations to provide automation procedures like (**SPM**) Security Policy Management, **SIEM**, (**NDR**) Network Detection and Response, (**EDR**) Endpoint Detection and Response, (**XDR**) Extended Detection and Response, Firewalls, Active Devices, (**CTI**) Cyber Threat Intelligence, Ticketing Systems and many others which aloows API to API communication, syslog or webhook data transport or even provides support for EDL (External Dynamic Lists).

Built-in integrations

paloalto NETWORKS · Check Point SOFTWARE TECHNOLOGIES LTD. · FORTINET · SOPHOS · Flowmon A Kemp Company · IBM QRadar · SURICATA · Office 365 · aws · NIST · VIRUSTOTAL · ipstack · SHODAN · ipinfo.io · MA:CV:en:do:rs