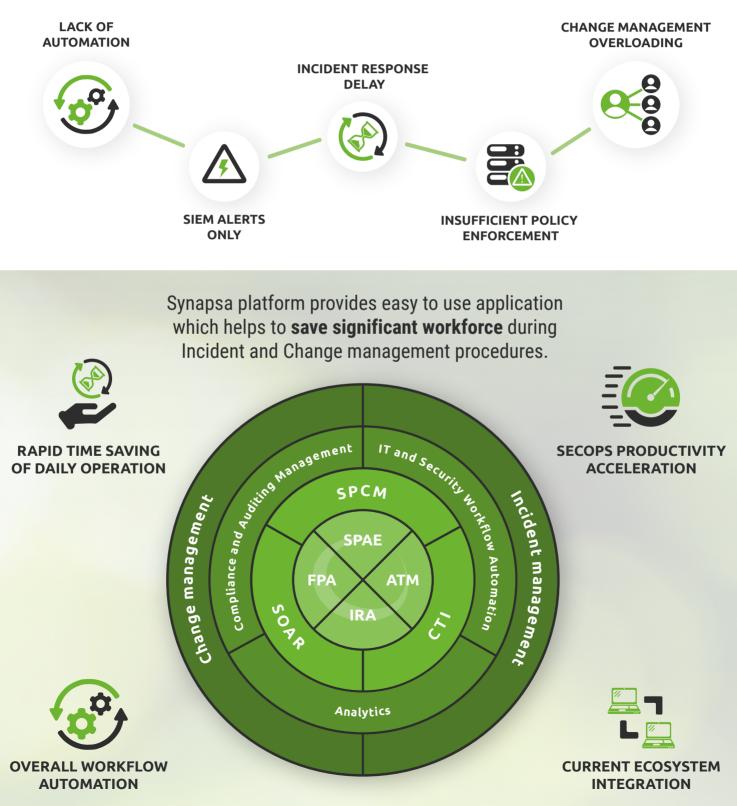


CYBER SECURITY AUTOMATION

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

Today's daily operation challenges



SYNAPSA PLATFORM

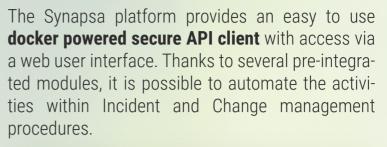
In the age of digital transformations, the increase in **cyber security threats**, alerts, daily operational tasks and the lack of sufficient resources, automation is one of the most effective options for ensuring critical **services availability** as well as **business continuity**.



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.



NAPSA								2 👁 🍕 🍠
RULES								@~
Name	Hiner	Fireval	Made	Ust	Allow List	Deny List	Allow threats	Delete
 Command and Control 	Flawman A23	DM2 FW 1 BA	Automat					
Active 🔴								
Cal (ECCE)	(PORTIGNAMMENT) (PORTIGNAMMENT) (PORTIGNAMMENT/MORY) (PORTIMANTANIT) (PORTIGNAMMENT)							
Rolback	alara latariy falay							
Description C&C								
Member Timeout								
Hitcount 4 🛢								
✓ Data Encryption	Flowmen ADS	DC CHCP PW 1 KE	Automat				(PARTITION)	
A Latend Movement	Flowmon ADS	Core PAN FW 1 BA	Manual					
Active 😐								
Call ·								
Rollback ·								
Description Lateral I	lovement							
Member Timeout 3600								
Hitcount 3 💼								
V Ordertal Access	Flowmon A05	Core PAN FW 1 BA	Manual	Malicious IP advesses			(1223)	

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 decisionmaking process and focus more on other necessary steps in daily operation.



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**.

375	YNAPSA		🖲 🏟 🕀 🚊 🔿
=	URL LIST - Phishtank		
0.0	Contex (Productional)		
ス勝	Ur	Cel 1	Col 2
3	Ntg. (Tombard 11. au/algoin.htm	http://www.phishtank.com/phish_detail.php?phish_id=6876555	2820-12-05714:05:41+00:00
0	http://dvla.mywhicke-rebate.com/	http://www.phishtank.com/phish_detail.php?phish.id+6875997	2820-12-05782-03 28=00:00
0	https://ud53H557.xoph.su/Wirker/	http://www.phishtask.com/phish_detail.php?phish.id=7108233	2021-65-06719:37.45=00.00
8	Mtg./fbbcwtees.net/Segure/	http://www.phishtank.com/phish_detail.php?phish_id=6875723	2820-12-04720-45 56+00-00
9	https://dd504557.coph.su/lifetoe	http://www.phishtank.com/phish_detail.php?phish_id+7108229	2821 65-06719:37.40+00:00
e l	https://inick.ees/Mpstae	http://www.phishtank.com/phish_detail.php?phish_id=6875714	2620-12-04720-28-03+00:00
8	http://w0004657.arsph.nu/Mitrae	http://www.phishtank.com/phish_detail.php?phish_id+7108228	202145-06719:37.34=00:00
۲	https://init/ee/judgemetrodus	http://www.phishtank.com/phish_detail.php?phish_id=6875793	2020-12-04720.24 15+00.00
œ	Mtgu:tu0509557.saph.nuffiirfae/	http://www.phishtank.com/phish_detail.php?phish_id+7108225	2021 65-06719:37:15+00:00
	https://kuse.edu.rp/morp/Drve/CD/Doc.htm	http://www.phishtank.com/phish_detail.php?phish_id=6875679	2820-12-04718-45-59+00:00
	http://amazon.user.auth.ylu2.top/	http://www.phishtank.com/phish_detail.php?phish_id+7100222	2021 65-06719:30 29+00:00
	Maps://docs.google.com/forms/she/1/ApdCU/bys/GU/GAAgu/CO/SEA/8_g8/CB/T/Oxf.Spg/n/%p308/5gCu/vee/form/v=-86-v64a+188/+66asp-mail_Sem_Enk	http://www.phishtank.com/phish_detail.php?phish_id+6875500	2820-12-04716:32:21+00:00
	Mgss./htadhparkasse-mail service.xyp1/u'anmeldung.php	http://www.phishtank.com/phish_detail.php?phish_id+7108213	2021 65 06719 30 08+00:00

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.



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.



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.



LOOK UP Cyber Threat Intelligence

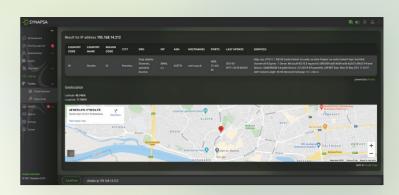
Allows to **fetch information** about IP, Domain, URL, hash, threat and more useful details from 3rd party services and correlate it with internal telemetry into the incident log.



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.

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.



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



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.

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).



www.synapsa.tech



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

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