www.synapsa.tech

FASTER RESPONSE

and Threat Mitigation to reduce impact

Speed up Incident Response





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.

TODAY'S DAILY OPERATION CHALLENGES



LACK **OF AUTOMATION** Not enough resources to asses



all important events

Long delay between threat detection and mitigation

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 SecOps productivity acceleration



Significant workforce savings in

daily Security, Network and IT

operation



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

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

FTE SAVINGS

Operation

Significant workforce savings within daily IT and Security

AUTOMATION

dent Management

Built-in intelligence simplifying

Compliance Check, Threat and Inci-

info@synapsa.tech





INCIDENT RESPONSE



CHANGE MANAGEMENT OVERLOADING

Manually solving tasks is highly time consuming

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

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.



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.



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.



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).

In the age of digital transformations, the increase in 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.

								∎ 🏶 🕀 La
RULES								ď~
Name	Hiner	Freval	Hode	List	Allew List	Deny List	Allow threats	Delete
Command and Control	Flowmon ADS	042 FW 1 BA	Automat					
ie 🔸								
Contractor of				0010010				
lack COLECTION								
crigities CBC								
nber Timeout								
ount 4 🛢								
Data Encryption	Flowmon ASS	DC CHCP FW 1 KE	Automat				(FREERE)	
Lateral Movement	Reemon ADS	Care PAN FW 1 BA	Manual					1.1
ne 🛛 🛛								
lack -								
cription Lateral Waveme	nt.							
aber Timeout 3600								
ount 3 B								

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).

NAPSA					∎ 🌻 ⊕ L
Ruferet CVE					
Active Confirmed Fixed					
Ruleset Alert detail					
Auditor		reval			
Portrange 50	•)	Deckport/102		•)	Fix Confir
Created_at	Security policy	Src addr	Dut eddr	Senica	Action
2021-05-04 23:35:16	BitTorrent	***	any .	Nappler_Client_6603-6699/5603-6699	Accept
8 B (2)					

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 vou vulnerable.

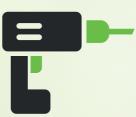
SYNAPSA		
URL LIST - Phishtank		
Custan (Produlined)		
и	Gett	CaliZ
http://fombard11.eu/signin.htm	http://www.phiahtank.com/phiah_detail.php?phiah_id=6879555	2020-12-05714-05-41+00-00
http://dvla.mywhicle-orbans.com/	http://www.phishtank.com/phish_detail.php?phish_id=6875987	2825-12-05782-03-26-00-00
https://d538557.segh.ex/lifeter/	http://www.phishtank.com/shink_detail.php?phish_id=7108230	2821-65-36719:37:45-30:00
Mtg./Mbcwtoes.net/Regun/	http://www.phishtank.com/phish_detail.php?phish_id=6875723	2820 12-04720 45 56+00:00
Mtgs::/v8539527.xgh.ru%Hrbe	http://www.phinhtank.com/phinh_detail.php?phinh_id=7108229	2821 65-06719:37-40-00:90
https://links.en.Wepdan	http://www.phiahtank.com/phiah_detail.ptp?phiah_id=4875774	282512-04720-29-03-00-00
http://dd594637.seph.ru/Mrise	http://www.phishtank.com/phish_detail.php?phish_id=7108228	282145-36719:3736-00:00
https://finitizes/pubgeneticulus	http://www.phishtank.com/yhink_detail.php?yhink_id=6875713	2825-12-54720.24 15+00.00
D Intputio050553 suph welfafree/	http://www.phishtank.com/phish_detail.php?phish_id=7108225	2821 65 06719 37 15400 00
https://wsee.edu.spilmorg/Gevu/CD/Goc.htm	http://www.phishtunk.com/phish_detail.php?phish_id=4875673	2025-12-04710-45 59+00-00
http://www.com.auth.giu2.10p/	http://www.phishtank.com/phish_detail.php?phish_id+7108222	282145-06719:30:29+00:00
Mgs.:/docs.google.com/forms/dre/17ApQL3hgwGx3AAbpcQfsEAdg62DCT0H_QgbHrfqDBHgExAviewfarm/hcr-blar-blar-blars_mail_torm_link	http://www.phishtank.com/phish_detail.php?phish_id=6875500	2829-12-64716-32-21-00-90
https://itadhpakassemail.senice.npz/v/anneldung.php	http://www.phishtank.com/phish_detail.php?phish_id=7108219	2021-05-06719-30-08-00-00

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 guery 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.

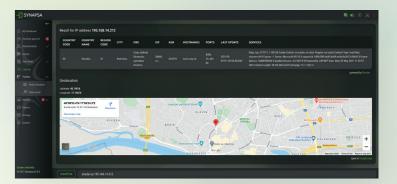


TOOLBOX Threat and Policy Testing

User can provide a **simulation** of what will be the Moreover user can **test** if a specific packet is allowed impact of a specific **threat** sent by a miner including all on the selected device's **ruleset** and which rule allows the actions as the threat is really reported. 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 com-**Speed-up mitigation time 10x** within Cybersecurity plete overview of Compliance Status in the Incident and Threat Management procedures dashboard widgets aggregated for all the monitothanks to Synapsa Platform smooth deployment, red devices, or individually for each asset to elimi- built-in integrations and parsers, custom rules and nate over 90% of the time spent on Audits. Moreo- actions. Improve data feeds management and high ver, it allows Continuous Monitoring and Automated speed data lookup techniques to decrease manual Remediation to ensure assets are always in complitasks with no alert fatigue and analyst burnout ance within CIS or other industry benchmarks. within the whole year 24/7.





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).

SYNAPSA									۲	¢:⊕ & O
	POLICY TES	TER								
😂 Analog spored 🛛 🔳										
	Frend				Show All					
B) Autor B) Des Note	Core PAN FW 1 BA				No					
G Lost op										
P* Taster	LAN									
	Destination Zone				Destination lp		Destination port			
🕼 MANDER 🛛 🖉 🗸	Internet				4523.145.12		22			
	The real									
	Protocol				Calegory		Application			
	TOP									
	_									
	Test									
										alex
Guides and help © 2021 Synepse v2.0.2	Constantine									