www.synapsa.tech SYNAPSA

SYNAPSA
Cyber Security Automation

CYBER SECURITY AUTOMATION

Save significant workforce in **security operation**, 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

LACK OF AUTOMATION
SIEM ALERTS ONLY
INCIDENT RESPONSE DELAY
INSUFFICIENT POLICY ENFORCEMENT
CHANGE MANAGEMENT OVERLOADING

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.

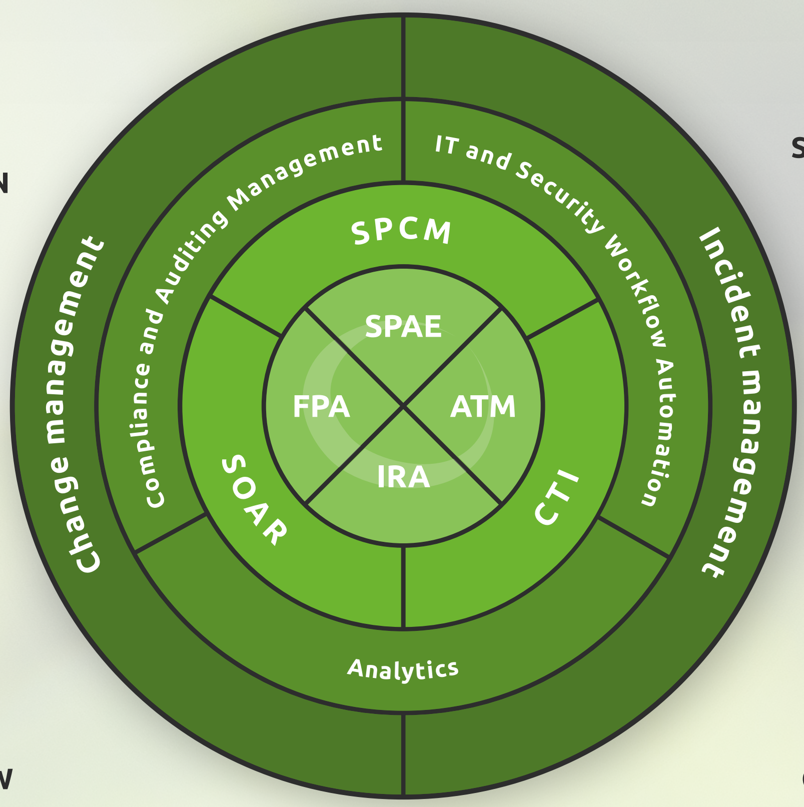
The platform provides an environment that automatically interconnects devices and tools in IT infrastructure to **simplify and speed up the processes** in real time, to continue audit and control of policies setup and their enforcement and lastly, to **prevent human failures**.

info@synapsa.tech

Synapsa 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


Change management
Incident management
Compliance and Auditing Management
IT and Security Workflow Automation
SPCM
SPAE
FPA
ATM
IRA
SOAR
CTI
Analytics

OVERALL WORKFLOW AUTOMATION

CURRENT ECOSYSTEM INTEGRATION

SYNAPSA PLATFORM

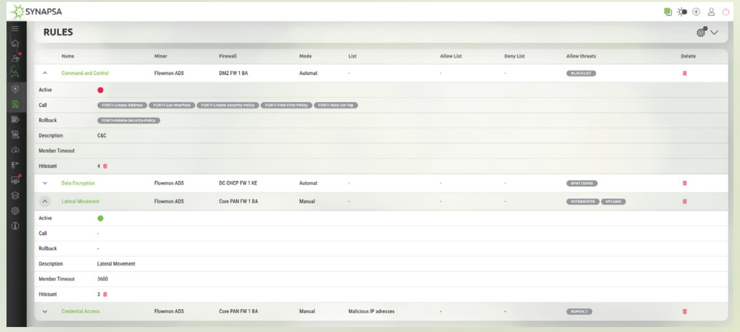
In the age of digital transformations, the increase in **cyber security threats**, alerts, daily operational tasks and the lack of sufficient resources, automation is one of the most effective options for ensuring critical **services availability** as well as **business continuity**.

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.



SYNAPSA

RULES

Name	Miner	Firewall	Mode	List	Allow List	Deny List	Allow threats	Delete
Command and Control	Flowmon ADS	DMZ FW 1 BA	Automat	-	-	-	BLACKLIST	
Data Encryption	Flowmon ADS	DC CHCP FW 1 KE	Automat	-	-	-	BPATTERNS	
Lateral Movement	Flowmon ADS	Core PAN FW 1 BA	Manual	-	-	-	HITRANSFER UPLOAD	
Credential Access	Flowmon ADS	Core PAN FW 1 BA	Manual	Malicious IP adresses	-	-	RDPDICT	

Command and Control:

Active	●
Call	FORTI-Create-Address FORTI-Get-Interface FORTI-Create-Security-Policy FORTI-Find-First-Policy FORTI-Rule-On-Top
Rollback	FORTI-Delete-Security-Policy
Description	C&C
Member Timeout	
Hitcount	4

Lateral Movement:

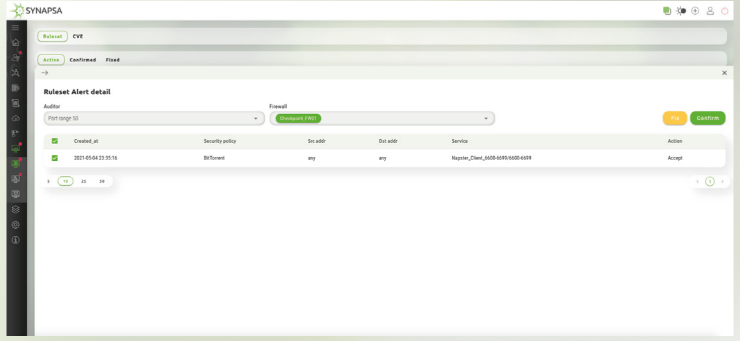
Active	●
Call	-
Rollback	-
Description	Lateral Movement
Member Timeout	3600
Hitcount	3

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.



SYNAPSA

Ruleset CVE

Active Confirmed Fixed

Ruleset Alert detail

Auditor: Port range 50

Firewall: Checkpoint_FW01

Fix Confirm

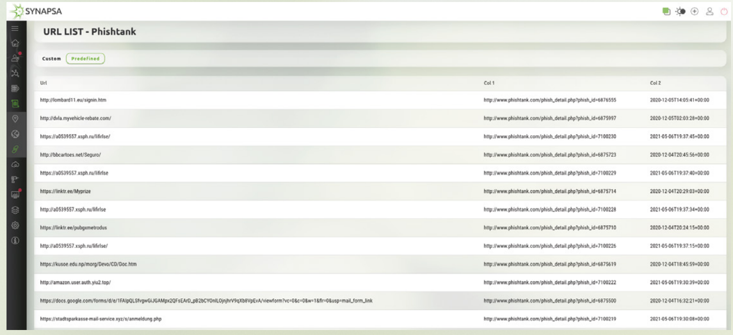
☑	Created_at	Security policy	Src addr	Dst addr	Service	Action
☑	2021-05-04 23:35:16	BitTorrent	any	any	Napster_Client_6600-6699/6600-6699	Accept

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.



SYNAPSA

URL LIST - Phishtank

Custom Predefined

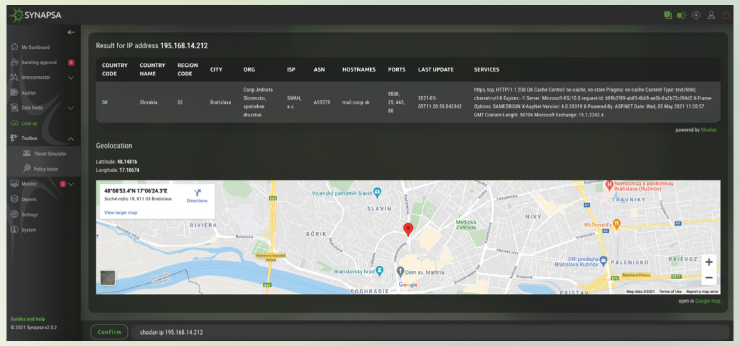
Url	Col 1	Col 2
http://lombard11.eu/signin.htm	http://www.phishtank.com/phish_detail.php?phish_id=6876555	2020-12-05T14:05:41+00:00
http://dvla.myvehicle-rebate.com/	http://www.phishtank.com/phish_detail.php?phish_id=6875997	2020-12-05T02:03:28+00:00
https://a0539557.xsph.ru/lifirlse/	http://www.phishtank.com/phish_detail.php?phish_id=7100230	2021-05-06T19:37:45+00:00
http://bbcartoes.net/Seguro/	http://www.phishtank.com/phish_detail.php?phish_id=6875723	2020-12-04T20:45:56+00:00
https://a0539557.xsph.ru/lifirlse	http://www.phishtank.com/phish_detail.php?phish_id=7100229	2021-05-06T19:37:40+00:00
https://linktr.ee/Myprize	http://www.phishtank.com/phish_detail.php?phish_id=6875714	2020-12-04T20:29:03+00:00
http://a0539557.xsph.ru/lifirlse	http://www.phishtank.com/phish_detail.php?phish_id=7100228	2021-05-06T19:37:34+00:00
https://linktr.ee/pubgxmetrodus	http://www.phishtank.com/phish_detail.php?phish_id=6875710	2020-12-04T20:24:15+00:00
http://a0539557.xsph.ru/lifirlse/	http://www.phishtank.com/phish_detail.php?phish_id=7100226	2021-05-06T19:37:15+00:00
https://kusoe.edu.np/morg/Devo/CD/Doc.htm	http://www.phishtank.com/phish_detail.php?phish_id=6875619	2020-12-04T18:45:59+00:00
http://amazon.user.auth.yiu2.top/	http://www.phishtank.com/phish_detail.php?phish_id=7100222	2021-05-06T19:30:39+00:00
https://docs.google.com/forms/d/e/1FAIpQLSfvgwGiJGAMpx2QFsEArD_pB2bCYOnlLOjnjhrV9qXb8VpEvA/viewform?vc=0&c=0&w=1&flr=0&usp=mail_form_link	http://www.phishtank.com/phish_detail.php?phish_id=6875500	2020-12-04T16:32:21+00:00
https://stadtsparkasse-mail-service.xyz/s/anmeldung.php	http://www.phishtank.com/phish_detail.php?phish_id=7100219	2021-05-06T19:30:08+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.

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.



SYNAPSA

Result for IP address 195.168.14.212

COUNTRY CODE	COUNTRY NAME	REGION CODE	CITY	ORG	ISP	ASN	HOSTNAMES	PORTS	LAST UPDATE	SERVICES
SK	Slovakia	02	Bratislava	Coop Jednota Slovensko, spotrebne druzstvo	SWAN, a.s.	AS5578	mail.coop.sk	8008, 25, 443, 80	2021-05-05T11:20:59.043342	https, tcp, HTTP/1.1 200 OK Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html; charset=utf-8 Expires: -1 Server: Microsoft-IIS/10.0 request-id: 689b2f89-ab85-4b69-ae3b-8a2b72cf04d2 X-Frame-Options: SAMEORIGIN X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Wed, 05 May 2021 11:20:57 GMT Content-Length: 58706 Microsoft Exchange: 15.1.2242.4

powered by Shodan

Geolocation

Lattitude: 48.14816
Longitude: 17.10674

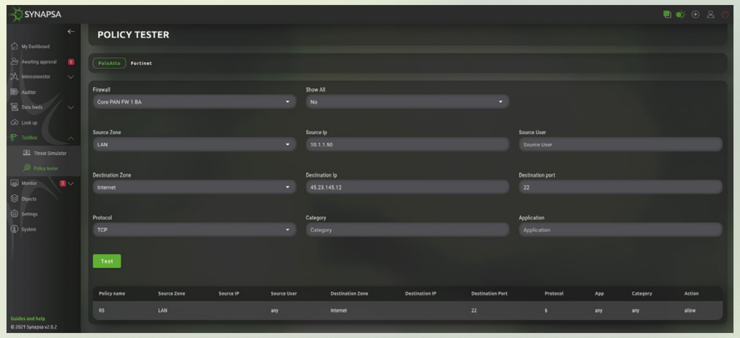
Confirm shodan ip 195.168.14.212

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.



SYNAPSA

POLICY TESTER

PaloAlto Fortinet

Firewall: Core PAN FW 1 BA
Show All: No
Source Zone: LAN
Source Ip: 10.1.1.50
Source User: Source User
Destination Zone: Internet
Destination Ip: 45.23.145.12
Destination port: 22
Protocol: TCP
Category: Category
Application: Application

Test

Policy name	Source Zone	Source IP	Source User	Destination Zone	Destination IP	Destination Port	Protocol	App	Category	Action
R5	LAN		any	Internet		22	6	any	any	allow

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