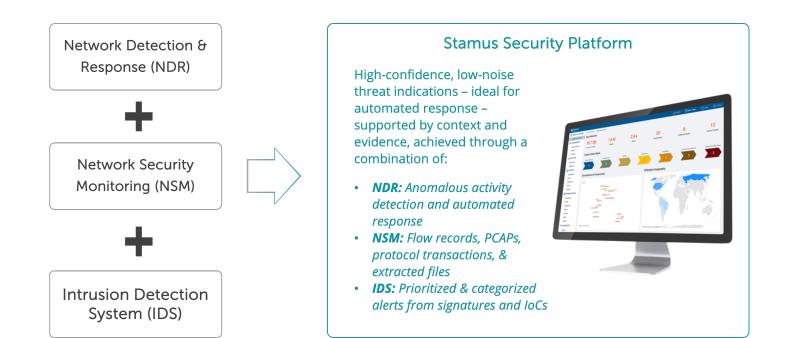
Expose serious threats and unauthorized activity lurking in your network.

With network-based threat detection and response solutions from Stamus Networks





Stamus Security Platform<sup>™</sup> (SSP) is an open network detection and response solution (NDR) built on a Suricata foundation that delivers actionable network visibility and powerful threat detection.



## Why Stamus Security Platform



Greater visibility into threat & network activity - Uncover even the weakest attack signals and unauthorized activity



**Transparent detections with evidence** - Know exactly what triggered an event with a detailed attack timeline & evidence



**Open and extensible for your environment** - Incorporate third-party threat intel. Easily integrate into your tech stack



**Built for enterprise-scale operations** - Scale to multi-site, multi-100Gbps deployments while tracking millions of hosts



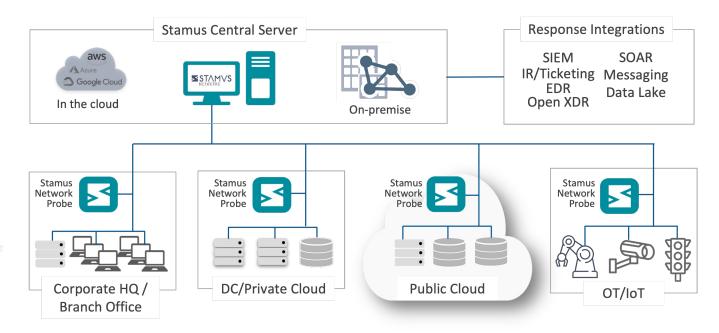
**Optional air-gapped deployment** - Deploy advanced analytics in the cloud or on premise – even in a completely air-gapped environment



Our probes or your Suricata sensors - Start with your Suricata sensors, transition to more advanced Stamus probes

Stamus Security Platform<sup>™</sup> (SSP) is an open network detection and response solution (NDR) built on a Suricata foundation that delivers actionable network visibility and powerful threat detection.

By combining the best capabilities of intrusion detection systems (IDS), network security monitoring (NSM), and network detection and response (NDR), the Stamus Security Platform is a new generation of NDR that helps organizations know more, respond sooner, and mitigate risk.



Stamus Security Platform consists of two components: Stamus Network Probe(s) and Stamus Central Server, which may be deployed in private cloud, public cloud, onpremise, or hybrid environments.

					🙏 Acme-Corporation	last 24 hours	⑦ Help	Scirius
I. SECURITY POSTURE	SECURITY POSTURE > OPERATIONAL CENTER							
Operational Center	Key Indicators							
COMPROMISES								
Impacted Assets	40.2 MB	6.7 k	822	7	2		6	
Timeline	Analyzed Traffic	Events	Alerts	Declarations	Impacted	Assets	Active Th	nreats
Coverage								
S ANALYTICS	Description	_						
Beaconing Sightings	Total volume of network traffic analyzed by the We	Kill Chain Chang	ges & Threats	Instal	lation Comm	and and Control	Actions on 0	Objectives
	Stamus Network Probes over the displayed period	2022-11-30 06:14:55 🚊	New hostname seen			0	2	
Dashboards								
Alerts		2022-11-30 06:15:07 🌐	New HTTP agent seen Microsoft NCSI					
Signatures	Declarations of Compromise			's Geography				
Hosts	(?)	2022-11-30 06:15:10 A	New user seen marlo.zaragoza@phantasmedia.com			-		
Policies					9 1 San 1			
ADMINISTRATION	Pow	2022-11-30 06:15:16 0	MalDoc switched asset to Delivery		A STAN	125		
Monitoring								
RYOD		2022-11-30 06:15:35 0		100	-		15.	
Appliances			Command and Control			7 4	S.A.	
Users		2022-11-30 06:15:35 🌐					K-M	
Sources			Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Ge	icko		1		
Other		2022-11-30 06:16:03 🗄						
History			<b>JA3 hash</b> 4d7a28d6f2263ed61de88ca66eb011e3				7	a de la calencia de l
الإمليم فيتعد		2022-11-30 06:16:03 0	Ursnif switched asset to Actions on Objectives		* * * * * *			
		2022-11-30 06:16:15 🍈	New HTTP agent seen Mazilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)				•	••••
: // ! ! !		2022-11-30 06:16:17	New TLS agent seen JA3 hash 6734/3743167063a6429258/60/29984					

## Stamus Networks – the global leader in enterprise class Suricata-based network security

Stamus Networks helps enterprise security teams accelerate their response to threats with solutions that uncover serious and imminent risk from cloud and on-premise network activity. Our advanced network detection and response (NDR) systems expose threats to critical assets and empower your rapid response.

## Trusted by the most-targeted organizations in the world



Government CERTs



Global Central Banks



Insurance Providers



Managed Service Providers



Multinational Gov't Institutions



Financial Institutions



Software

Cybersecurity Vendors

## Proven in NATO Cybersecurity Exercises



For the past five years, Stamus Networks and SSP have been invited by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) to join their annual Locked Shields and Crossed Swords exercises where we refine and validate our latest threat detection capabilities.

> www.Stamus-Networks.com CORP-SSP-052024-1 Copyright © 2023