



NEXT-GENERATION BEHAVIORAL ANALYTCS WITH PRO-ACTIVE DEFENSE

The **Fortinet** Security Fabric platform provides true integration and automation across an organization's security infrastructure, delivering unparalleled protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises.

LinkShadow® Cyber Security Analytics Platform is designed to manage threat in real-time utilizing Artificial Intelligence-based Machine Learning to analyze events, performs UEBA, and cutting-edge Threat Hunting & provides threat anticipation.

LinkShadow® provides unparalleled detection of the most sophisticated threats which enhances an organization's defense against advanced cyber-attacks, zero-day malware and ransomware. The chance of an attacker passing through your network is virtually nonexistent.

INTEGRATION STORY: LINKSHADOW - FORTINET

- LinkShadow® integrates with Fortinet and completes the full cycle of User and Entity Behavioral Analytics and Threat Hunting to get the optimum benefit of Fortinet Enterprise technology along with proactive threat detection.
- LinkShadow gets full visibility from Fortinet Enterprise around system change activities. This
 intelligence is injected into the Advanced Machine Learning Algorithms to identify suspicious and
 anomalous activities based on the behavioral analysis. LinkShadow acts proactively to system change
 activities that might indicate an early stage of an attack for faster resolution and forensic value.
- LinkShadow integrates with Fortinet FortiGate Firewall to accommodate highly automated, complex incident response, delivering faster results and facilitating an adaptive defense against most sophisticated and unknown attacks.

JOINT COMPONENTS:

FortiMail, FortiProxy, FortiSIEM FortiSOAR, FortiWeb, FortiGate

HIGHLIGHTS:

- Seamless Integration to Automate the Incident Response
- » High-level Insights into Security Investments
- Proactive Prevention against Behavioral Anomalies
- Defense against Unknown Attacks in Early Stages

JOINT USE CASE

Compromised System Early Detection and Response

Although attacks can be detected in early stages by monitoring the TTPs; zero-day and unknown attacks remain undetected till it is too late. Instead of sleeping on anomaly till it poses a real threat, LinkShadow monitors the connections to the external network for each profile individually. LinkShadow has full visibility up to the application layers, which allows it to monitor unusual or abnormal connections and data exfiltration. LinkShadow communicates with FortiGate to proactively stop the anomaly before it poses any threat!

		Туре		Description					S	core		Time				
		Unusual Connection		Started at: 2019-10-01 17:13:10						27)		2019-10-01 1				
				2019-10-01 17:	14:10 Co	enection not seen	t seen before						Action			
						Unusual connection detected at this time Unusual connection detected at this time		time					-	Actions		
				2019-10-01 17:				ed at this time					N	ormal Beha	avior	
													Ad	d to Truste	d List	
	All Events	Anomalies	∑ Stages	E MITRE ATT&	CK MATRIX	:									Reset	t F
- 1 <u>†</u>	• •		• • • •	• • •	••	••••			•	• ••	••	• ••	••	•••		•
		02:15	62:20	02:25		02:30	02:30		02:40		02:45		02:50		02.55	_
	02:10	02:15	62:20	02:25		02:30	023		0240		02:45		02:50		a2.55	
		02:15	02-20 02-20	02:25					0240		02:45		02:50			
	- 11°			02:25		02:30	02.3		02:40						• •	
P-	02:10			02:25			02.3		02:40			• ••		Search:	• •	
	02:10	<u></u>	02:20	02:25		oziso naly Recent	Anomaly		0240	. :.	02545				02:55	
	02:10	ou d' es o o oz:15 Log Source	cc:20 Source	•* •• •• 02:25 • 50	Source I	oziso naly Recent	Anomaly	Recent Event	0240		02545 Destinatio				• •	•
	02:10 v entries 2 ± Time 2019-10-01	<u></u>	02:20	•* •• •• 02:25 • 50		oziso naly Recent	Anomaly		0240		02545				02:55	•
	02:10 v entries a 4 Time 2019-16-01 14:07:53	co:15 Co:15 Log Source Dynamic Protocol	02:20 Source 172.16.60	•• •• 0225 • 5 IP	Source I	oziso naly Recent	Anomaly P	Recent Event estination IP 194.195.222	0240		02:45 Destinatio				colss Event View Data	
	02:10 v entries 2 ± Time 2019-10-01	ou d' es o o oz:15 Log Source	cc:20 Source	•• •• 0225 • 5 IP	Source I	oziso naly Recent	Anomaly P	Recent Event	0240		02545 Destinatio				coss Event	
	02:10 entries	215 02:15 02:15 Log Source Dynamic Protocol Dynamic Protocol	02:20 Source 172:16:60	•* •• •• 0225 • 5: IP 103	Source 1 59700 59704	oziso naly Recent	** 02:30 Anomsiy • 23. 23.	** Recent Event estination IP 194.195.222 194.195.222	0240		02545 Destination				c2:55 Event View Data	1
	02:10 CO2:10	co:15 Co:15 Log Source Dynamic Protocol	02:20 Source 172.16.60	•* •• •• 0225 • 5: IP 103	Source I	oziso naly Recent	** 02:30 Anomsiy • 23. 23.	Recent Event estination IP 194.195.222	0240		02:45 Destinatio				colss Event View Data	1
	02:10 v entries t t t t t t t t t t t t t t t t t t t	215 02:15 02:15 Log Source Dynamic Protocol Dynamic Protocol	02:20 Source 172:16:60	• • • • • • • • • • • • • • • • • • •	Source 1 59700 59704	oziso naly Recent	** 02.9 Anomaty • 23. 23. 23.	** Recent Event estination IP 194.195.222 194.195.222	0240		02545 Destination				c2:55 Event View Data	•
	02:10 02:10 02:10 019:10:01 14:07:54 2019:10:01 14:07:54 2019:10:01	C215 Log Source Dynamic Protocol Dynamic Protocol	62:20 Source 172.16.60 172.16.60	103 0225	Source 1 59700 59704 61362	oziso naly Recent	* 02.% Anomaly • 23. 23. 23. 23.	Recent Event estination IP 194.195.222 194.195.222	0240		02:45 Destination 10				Co.55 Event View Data View Data	1
	••••••••••••••••••••••••••••••••••••	C215 C215 Log Source Dynamic Protocol Dynamic Protocol Dynamic Protocol	02:20 Source 172:16:00 172:16:00 172:16:00	····································	Source 1 59700 59704 61362 51532	oziso naly Recent	* 02.95 Aromsly • 23. 23. 23. 23. 23. 24. 24. 24. 24. 24. 24. 24. 24. 24. 24	Recent Event estination IP 194, 195, 222 194, 195, 222 194, 195, 222 194, 195, 223	0240		02245 Destination 10 10 10				C255 Event View Data View Data	1 1 1



