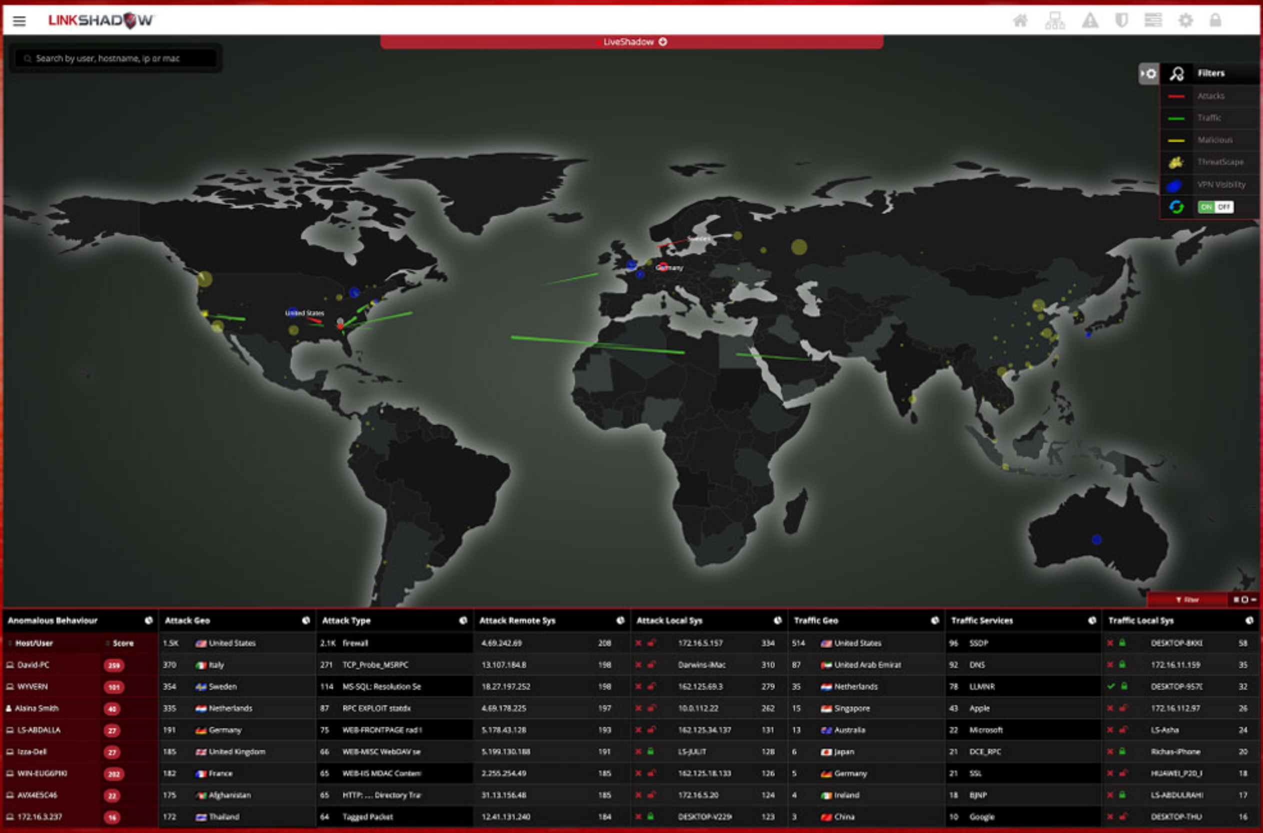
LINKSHADOW®
Combat the Dark

MODERNIZE YOUR SOC WITH EXTENDED THREAT HUNTING AND RESPONSE

Detect Cyber and Insider Threats

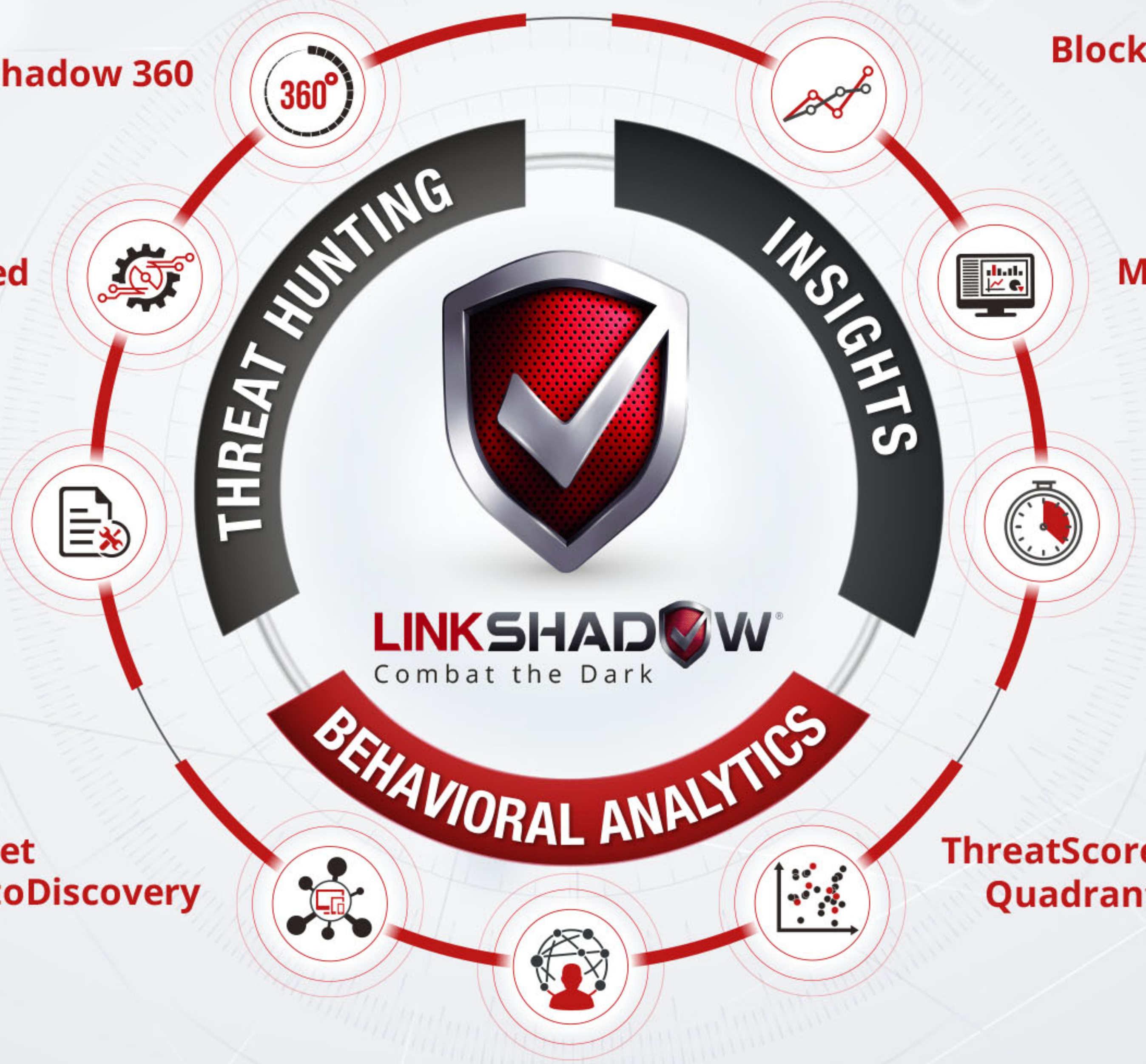
www.linkshadow.com

LINKSHADOW, NEXT-GENERATION CYBERSECURITY ANALYTICS.



Anomalous Behaviour		Attack Geo		Attack Type		Attack Remote Sys		Attack Local Sys			Traffic Geo		Traffic Services		Traffic Local Sys		
Host/User	Score	1.5K	United States	2.1K	firewall	4.69.242.69	208	✗ 🔓	172.16.5.157	334	514	United States	96	SSDP	✗ 🔒	DESKTOP-8KKI	58
David-PC	259	370	Italy	271	TCP_Probe_MSRPC	13.107.184.8	198	✗ 🔓	Darwins-iMac	310	87	United Arab Emirat	92	DNS	✗ 🔒	172.16.11.159	35
WYVERN	101	354	Sweden	114	MS-SQL: Resolution Se	18.27.197.252	198	✗ 🔓	162.125.69.3	279	35	Netherlands	78	LLMNR	✓ 🔒	DESKTOP-957I	32
Alaina Smith	40	335	Netherlands	87	RPC EXPLOIT statdx	4.69.178.225	197	✗ 🔓	10.0.112.22	262	15	Singapore	43	Apple	✗ 🔓	172.16.112.97	26
LS-ABDALLA	27	191	Germany	75	WEB-FRONTPAGE rad I	5.178.43.128	193	✗ 🔓	162.125.34.137	131	13	Australia	22	Microsoft	✗ 🔓	LS-Asha	24
Izza-Dell	27	185	United Kingdom	66	WEB-MISC WebDAV se	5.199.130.188	191	✗ 🔒	LS-JULIT	128	6	Japan	21	DCE_RPC	✗ 🔒	Richas-iPhone	20
WIN-EUG6PIKI	202	182	France	65	WEB-IIS MDAC Conten	2.255.254.49	185	✗ 🔓	162.125.18.133	126	5	Germany	21	SSL	✗ 🔓	HUAWEI_P20_I	18
AVX4E5C46	22	175	Afghanistan	65	HTTP: .... Directory Trar	31.13.156.48	185	✗ 🔓	172.16.5.20	124	4	Ireland	18	BJNP	✗ 🔒	LS-ABDULRAHI	17
172.16.3.237	16	172	Thailand	64	Tagged Packet	12.41.131.240	184	✗ 🔒	DESKTOP-V229	123	3	China	10	Google	✗ 🔓	DESKTOP-THU	16

Designed to manage threats in real-time with attacker behavioral analysis, **LinkShadow** is meant for organizations that are looking to enhance their defenses against advanced cyberattacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.



Shadow 360

Obtain in-depth view of all activities before and after an anomaly

BlockCount Ratio

Validate the effectiveness of existing security solutions and their ROI

AI-Powered Engine

Manages end-to-end from data collection to detection and visualization

Management Dashboard

Overview of organizations' security posture providing high-level security KPIs & KRIs to CXOs

AML Anomaly Detection

Detect anomalies through advanced machine learning algorithms applied on enriched network & user data

LiveShadow

Compilation of all critical security findings in real-time

Asset AutoDiscovery

Automatically discover & track assets across the entire network and monitor activity trends

ThreatScore Quadrant

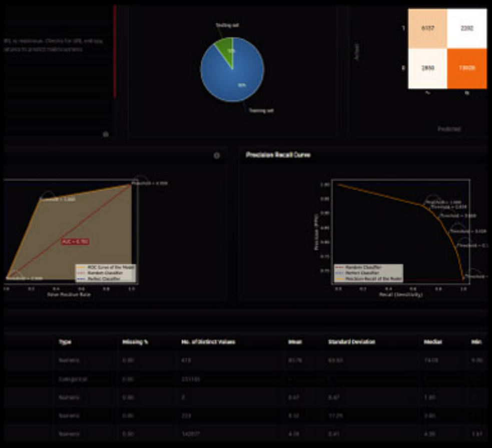
Learn, score and prioritize assets & users for action, based on risk scores

Identity Intelligence

Get visual trend analytics on user behavior including authentication patterns, application usage habits etc.

www.linkshadow.com

AI-Powered Engine



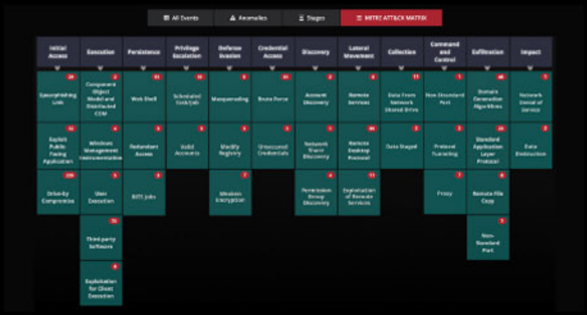
AI-Powered Engine is an end-to-end mechanism that enriches data for Advanced Machine Learning (AML) Anomalies Detection capabilities. It will empower the Enterprise to manage the whole process from data collection to detection and visualization, seamlessly. Simply, an Enterprise can collect data, create a Machine Learning model, build a data list, or upload a ready-to-use one, train a Machine Learning model, monitor its details, quality, and accuracy, and get detections visualised.

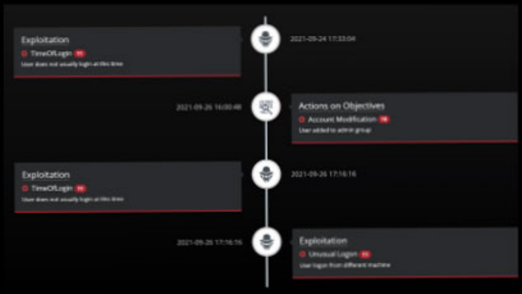
Remote Access Visibility

With the recent turn of events, work from home trend has increased the exposure of compromise along with network abuse by insider threats. LinkShadow provides visibility of the Remote Access patterns to your organization and finds the 'who', 'when', 'where' of their activities.

MITRE ATT&CK & Cyber Kill Chain Frameworks

Uncover the attackers TTPs with LinkShadow threat detections mapped to MITRE Framework. Identify which techniques are more prominently used in your environment with suggestions to mitigate. Help environment to thwart the attackers and strengthen Security Posture.





Exploitation
TimeOfLogin
User does not usually login at this time
2021-09-24 17:33:04

2021-09-26 16:00:48
Actions on Objectives
Account Modification
User added to admin group

Exploitation
TimeOfLogin
User does not usually login at this time
2021-09-26 17:16:16

2021-09-26 17:16:16
Exploitation
Unusual Logon
User logon from different machine

LINKSHADOW

Combat the Dark

Suite 444, 320 E Clayton Street, Athens, Georgia 30601, USA I T: +1 877 267 7313

info@linkshadow.com I www.linkshadow.com

October 2021