

LINKSHADOW 

Intelligent NDR Cyber Mesh Platform

— The New Approach to Cybersecurity Posture —



Get a clear view of your entire Cyber Security Posture

The screenshot displays the LinkShadow dashboard interface. At the top, there is a search bar and a 'Live Status' indicator. The main area features a world map with green and red lines indicating network connections and attacks. Below the map is a table with columns for various security metrics. To the right, there are panels for 'Endpoint - VMware Carbon Black Cloud' and 'Yara | Investigate | Rule', both showing 'Installed' status. At the bottom, there is a 'Tags' section with a list of categories and their counts.

Anomalous Behaviour	Attack Geo	Attack Type	Attack Remote Sys	Attack Local Sys	Traffic Geo	Traffic Services	Traffic Local Sys
Host/User Score	1.2K United States	2.1K Firewall Deny	8.8.8.8	576 172.16.88.71	1.2K 514 United States	95 SDDP	DESKTOP-80XG
David-PC 100	124 United Kingdom	16 IP Length Invalid, e.g.,	91.74.62.171	59 172.16.88.8	212 87 United Arab Emirat	92 DNS	172.16.11.159
Alaina Smith 29	80 Russia	13 WEB-MISC http directo	184.29.241.29	21 172.16.88.11	82 35 Netherlands	78 LLNMR	DESKTOP-957I
LS-ABDALLA 39	75 United Arab Emirat	12 MS-SQL Packet Bounc	4.2.2.2	18 172.16.88.25	76 15 Singapore	43 Apple	172.16.112.97
Izza-Dell 27	67 Romania	12 RPC EXPLOIT statdx	104.26.10.83	17 172.16.88.75	76 13 Australia	22 Microsoft	LS-Asha

Tags

- Action: 27
- SOAR: 3
- Incident: 3
- Respond: 3
- Apply policy: 2
- Endpoint: 19
- Yara: 1
- Investigate: 14

Endpoint - VMware Carbon Black Cloud
Status: Active
Version: 1.1
Description: VMware Carbon Black Endpoint Plugin is used for in ...
Endpoint: Installed

Yara | Investigate | Rule
Status: Inactive
Version: 1.9
Description: This Plugin Allows LinkShadow Users to capture the ...
Packet capture | Investigate: Installed

Enrichment - Azure Log Collection
Status: Active
Version: 2.3
Description: Azure Plugin is used for enabling Azure Log Integr ...
Azure | Active Directory | Investigate | logs: Installed

In today's rapidly evolving threat landscape, organizations require advanced cybersecurity solutions that provide comprehensive visibility, efficient incident response and seamless integration across various security tools. LinkShadow's intelligent Network Detection and Response (iNDR) offers a groundbreaking approach to cybersecurity architecture, leveraging the Cybersecurity Mesh Architecture (CSMA) to connect the dots and provide organizations with enhanced security posture. Intelligent NDR can help organizations improve their security defenses, reduce costs, and enhance overall efficiency.

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

Shadow 360



BlockCount Ratio

Validate the effectiveness of existing security solutions and their ROI

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

AI-Powered Engine



Management Dashboard

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

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

AML Anomaly Detection



LiveShadow

Compilation of all critical security findings in real-time

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

Asset AutoDiscovery



ThreatScore Quadrant

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

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

Identity Intelligence



Leveraging the Cybersecurity Mesh Architecture Approach

LinkShadow revolutionizes the way organizations approach cybersecurity. It emphasizes open architectures and standardization to facilitate seamless integration between individual security elements and centralized functions. CSMA promotes interconnectivity, allowing security tools to leverage data and intelligence from other tools and enterprise data sources. This approach improves overall visibility, threat intelligence sharing, and incident response capabilities.

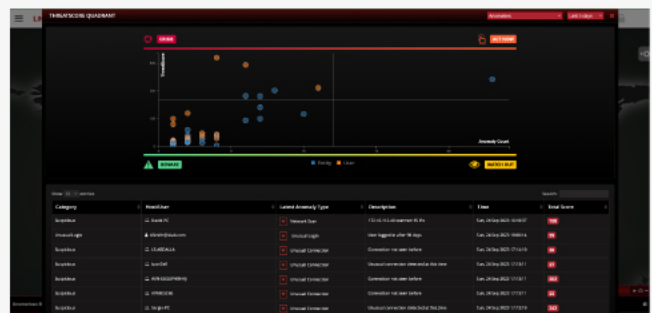
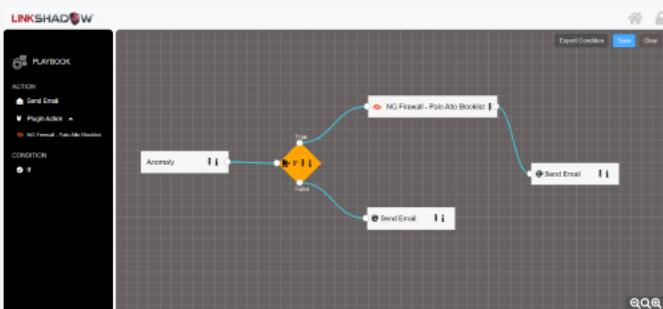


Cost Savings and Improved SOC Efficiencies

By implementing LinkShadow intelligent NDR, organizations can achieve significant cost savings. The solution streamlines security operations, reducing the need for manual intervention and minimizing staff costs. Additionally, the centralized policy management and aggregated threat data store enhance incident response capabilities, leading to improved SOC efficiencies.

Automated Response and Threat Prioritization

LinkShadow's AI and ML-powered engine automate the detection and response process, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The solution utilizes User Entity Behavior Analytics (UEBA) to identify anomalous user activities and prioritize threats based on their severity. This enables security teams to focus on critical threats and allocate resources efficiently.





REQUEST FOR A DEMO

USA - Headquarters:

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

Regional Offices:

UAE

Office 1606
Mazaya Business Avenue
BB2 JLT Dubai, UAE
P.O. Box 95679
T: +971 4 408 7555

UK

3rd Floor
12 Gough Square
London, EC4A 3DW
T: +44 20 4524 4205

KSA

P.O Box: 4055
Leaders 2 Tower, 6th Floor
Office 62, King Fahad Road
Riyadh - KSA
T: +966 11 456 6672

India

1st Floor
Carnival Infopark Phase 1
Infopark Campus, Kakkanad
P.O. Box 682042, Kochi - Kerala

Netherlands

Gustav Mahlerplein 2
1082 MA Amsterdam
The Netherlands
T: +31 20 225 3099