

## Industry

# LEADING FINANCIAL EXCHANGE

EMPLOYEES - 1000+

CASE STUDY

One of the leading financial exchange in the region who is focused on technology and innovation for enduring growth and diversification deployed LinkShadow solutions and services to protect and secure their Endpoint, Network, Assets, as well as for Incident Management and IT Risk Mitigation.

## CHALLENGES

**As a Financial organization, the customer faced a range of cyber security analytics challenges:**

- Insider threats can be particularly challenging for financial organizations where employees may have access to sensitive information and systems. There was a need to implement monitoring and access controls to detect and prevent insider threats.
- Inability to adhere to strict security standards and implement appropriate controls to mitigate the risks.
- Non-compliance to various regulations and standards related to cyber security. Meeting these requirements was challenging and required a comprehensive approach to cyber security analytics.
- SOC Team manages and maintains a vast array of cybersecurity products which are already equipped with the latest global threat detections, but they also want to tune these cybersecurity systems as per the local cyber threat feeds which they are subscribing. They were facing challenges in manual tuning of all their systems with the local threat feed on top of the vendor-provided Global threat feed.



## SOLUTION

LinkShadow intelligent NDR with its Advanced AI-based Analytics and UEBA helped customer address the cyber security analytics challenges it faces. LinkShadow provided with a range of benefits that can help to mitigate the risks associated with cyber threats. Some of the way Linkshadow helped include:

- LinkShadow can monitor suspicious activity by employees and contractors, helping customer to identify and prevent insider threats. Linkshadow provides visibility into user behavior, identify suspicious activity, and generate alerts in real-time.
- LinkShadow helped in meeting regulatory requirements and standards related to cyber security by providing a comprehensive approach to cyber security analytics. Linkshadow provided visibility into compliance with regulations and standards, generate compliance reports, and help to demonstrate compliance to auditors.
- Not only did LinkShadow's build-in Threat Intel Management module to help the Infosec Team to connect with DESC's threat feeds on a web API control and ingest the feed into local analysis of LinkShadow, but also distribute these feeds to other security solutions like firewalls and proxy devices and Endpoints.
- LinkShadow's unique threat intel management module can accept threat feeds from providers via Web API, or even static files as XLS, CSV or even PDF documents.

In summary, LinkShadow provided with enhanced threat detection, and visibility into security risks across its organization and achieve compliance. By implementing Threat Analytics Platform solution, it could improve its cyber security analytics capabilities and mitigate the risks associated with cyber threats.

## BENEFITS

Implementing LinkShadow intelligent NDR solution significantly improved the security status and posture of the customer. By providing enhanced threat detection it reinforced with global and local threat feeds as well as response capabilities. It also helped reduce the risk of cyber attacks and protect business operations, customers, and reputation. Some of the ways that LinkShadow helped improve the security status:

- LinkShadow Analytics Platform provided with enhanced threat detection capabilities that helped detect potential threats across the organization's networks, systems, and applications, plus feed the threat intel into the other security solutions and services maintained by customer.
- The iNDR module of LinkShadow can detect network-based threats, while UEBA can identify unusual user and entity behaviors that could be indicative of an attack.
- LinkShadow provided with faster incident response by automating incident response capabilities that quickly remediate threats before they can cause damage or data loss. Also supported to reduce the time to resolution and minimize the risk of damage or data loss.
- LinkShadow iNDR helped customer adopt a more proactive approach to cyber security by identifying and remediating security risks before they can be exploited by attackers. iNDR can detect suspicious activity in real-time, while UEBA can identify anomalies in user behavior that could indicate a potential security risk.
- LinkShadow iNDR provided with improved visibility into its security posture, including the ability to monitor and analyze user behavior, network traffic, and system activity. The solution's advanced analytics capabilities provided with actionable intelligence to improve its security posture.