LINKSHADOW

Industry

NATIONAL EDUCATION AUTHORITY

EMPLOYEES - 3000+

CASE STUDY

LinkShadow had the opportunity to work with a major Government Entity linked to the education sector whose vision is to enhance education and training professionals in both private and public sector in the region.

CHALLENGES

- Limited visibility to the network traffic. With no visibility on the users and entities within the centre for related activities and abnormal behaviours.
- Most of the existing security solutions are functioning and doing their job, But it lacked the synchronization between each other where each tool is operating separately.
- They needed a solution to focus on both known and unknown attacks - not to be only depending on known use cases and rules that we can write to discover the unknown area needs to be addressed.
- Their SOC teams spent most of their time in the investigation of false positives and noisy alerts as alerts are showing without any priority.
- Complicated interfaces giving our team hard time navigating around the solution to find a useful information, which is considered a very time and resources consuming and gives more time for a critical threat getting riskier.

SOLUTION & BENEFITS

LinkShadow intelligent NDR helped enhance the overall cybersecurity status for the customer and helped overcome most of the challenges in terms of Network visibility, Users Visibility, Assets Visibility that its facing and many other challenges that were solved and not limited to:

- LinkShadow provided deep visibility into the users and the user behavior. LinkShadow digs deep into the behavior of the Users involved in the anomaly and provides the Interactive logins activities, connections, peer group analysis, and more insights that will help in the investigation and the forensics.
- LinkShadow leveraged the integration with existing security tools, for extended functions and capabilities and even new features.
- LinkShadow used advanced machine algorithms for analytics to build a mathematical model of users and entities on a network (UEBA), looking for anomalies, score it based on various factors to then send it for investigation seamlessly and without any human interaction. LinkShadow also complies with MITRE ATT&CK, Cyber Kill Chain Framework and more to fully comprehend the threat landscape and make better use of the LoCs as part of the Intelligence Driven Defense, to document and track various techniques attackers use through.
- With LinkShadow, threat scoring methodology and prioritization is built in within the threat score quadrant, you can even toggle the sensitivity level of the detection to minimize the Noisy Alerts and possible False Positives and only get alerted for actual threats with a respective Risk Score.
- LinkShadow has an extremely user-friendly interface engineered and created by a team of developers with a SOC background. LinkShadow is built to make the SOC analyst life easier

CUSTOMER FEEDBACK

"Having LinkShadow in our premises definitely saved us plenty of time with its visibility, detection capabilities and its automation for the information gathering and visualization at the same time, Effective results on the time consumed from the SOC team through the daily cybersecurity operations"