LINKSHADOW®

How a Government Entity Enhanced Its **Cyber Posture with LinkShadow iNDR?**

OVERVIEW

A government organization with under 5,000 employees sought to enhance its cybersecurity posture and improve operational efficiency within its Security Operations Center (SOC). The organization needed a solution that could offer deep threat visibility, integrate seamlessly with existing tools, and deliver localized support.

Their Senior Network and Security Engineer, leading the IT Security and Risk Management function, was tasked with identifying a platform that combined powerful detection capabilities with ease of use. After a thorough evaluation, the organization selected LinkShadow iNDR.

INDUSTRY INSIGHTS

Industry: Government
Function: IT Security and Risk Management
Role: Senior Network and Security Engineer
Firm Size: <5,000 Employees

CHALLENGES

- Limited network visibility and fragmented threat insights
- Siloed tools creating gaps in response coordination
- False positives during early stages of behavioral analytics
- Lack of in-country support from existing vendors

RESULTS & BENEFITS

- ☑ Significantly improved SOC workflow efficiency
- ☑ Enhanced threat detection accuracy over time
- ☑ Reduced mean time to respond (MTTR)
- ☑ Increased visibility across user and entity behaviors
- ☑ Faster resolution with responsive in-country support

Why LinkShadow?

The organization selected LinkShadow iNDR due to:

- Comprehensive product capabilities, including UEBA, threat hunting, and network visibility

- Strong customer-centric approach and responsive in-country support Seamless bidirectional integration with existing SIEM and EDR tools

- A scalable platform with a clear, forward-thinking product roadmap

Implementation & Integration

Rated 5/5 for integration and deployment, the onboarding process was smooth and well-supported. LinkShadow's flexible architecture allowed rapid deployment without major workflow disruptions. The unified dashboard simplified monitoring and gave analysts a clear view of potential threats in real time.

Key Capabilities Used

- User & Entity Behavior Analytics (UEBA)
- Threat Hunting & Network Visibility
- Automated Alert Correlation
- Customizable Dashboards & Reporting
- Integration with Existing Security Tools

CONCLUSION

LinkShadow iNDR empowered this government entity to move from reactive to proactive cybersecurity. The platform's seamless integration, strong detection capabilities, and intuitive interface enabled the team to respond faster and work more efficiently. Combined with exceptional local support, LinkShadow continues to play a critical role in securing the organization's digital infrastructure.