CYBER DEFENSE CENTER
for Managed Threat Detection & Response

Service: Cybersecurity

OVERVIEW

The customer is a $2bn telecommunication service provider based out of India. With evolving cyber threats, they wanted to set up a Cyber defense center to define security incident management process.

CHALLENGES

Security incidents are not getting investigated properly due to lack of security professionals

Tools and processes were not scalable, and several data and tasks were scattered amongst various team members

Less visibility into threats & attack methodologies impacting the business

SOLUTION

Deployed SIEM and SOAR tools

1. Configured event correlation and management using Splunk
2. Splunk Phantom was introduced to consolidate all data sources and to automate routine tasks through multi-stage security orchestration
3. Data ingestion through Threat intelligence tool for external threat visibility and IOC's
4. Use cases are configured using Phantom playbook

OUTCOMES

- 100% Critical incidents resolved
- 3x Number of incidents resolved per shift

ACL Digital is a design led Digital Experience, Product Innovation, Engineering and Enterprise IT offerings leader. From strategy, to design, implementation and management we help accelerate innovation and transform businesses.

ACL Digital is a part of ALTEN group, a leader in technology consulting and engineering services.

To know more about how ACL can partner with you to help create Digital Transformation, connect with: **business@acldigital.com**

www.acldigital.com

USA | UK | France | India