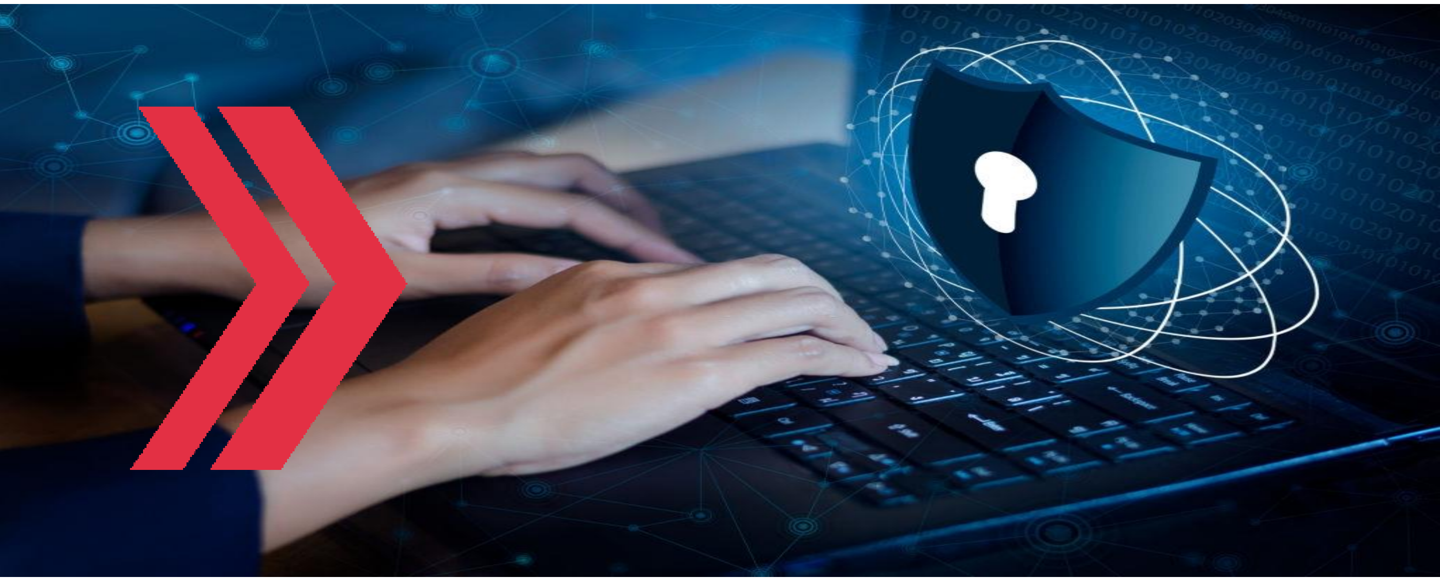
Connected World.
Connected Experiences.

Tech Mahindra

CASE STUDY

HOW A LEADING MOBILE TELECOM SERVICE PROVIDER IMPLEMENTED LARGE SECURITY OPERATION FOR NETWORK SECURITY DEVICES



BUSINESS CONTEXT

The Client aimed to enable Services – IT Security management and monitoring

- Security Event Management
- Incident Management
- Vulnerability Management
- Device Monitoring and Management
- Firewall Management
- Threat Advisories
- DR testing services
- Evaluation of new technology solution, Planning and Design
- Installation and Implementation

APPROACH AND SOLUTION

Technology Landscape

- Firewall/VPN: Cisco ASA, Checkpoint Gaia, Juniper, F5
- NIPS/HIPS: SourceFire, ArcSight, Checkpoint DLP
- Proxy/Content Filtering: Bluecoat Proxy SG/ AV/ Director
- Authentication (2FA): RSA ACE Server with a Replica
- End Point Protection: Symantec End Point Protection
- Mail Security: Checkpoint DLP/ IronPort
- SIEM: ArcSight

Metrics

- 1200 Total Service Calls processed
- 6000+ Operational Firewall rule sets
- 300+ Windows Application Servers installed with Endpoint Protection for Antivirus Management
- 80+ Site-to-Site VPN tunnels
- 60+ Published sites/web servers integrated with SIEM

IMPACT & HIGHLIGHTS

Brand Protection due to minimized risk from potential security exploits

Increased assurance on security posture through regular reports and dashboards to senior management

Proactive stance and increased resilience to zero day attacks through regular threat ad vulnerability advisories

Compliance to regulations and internal organizational policies

.

ESRM.Communications@TechMahindra.com

Tech Mahindra

Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.