

## **India's Reputed Financial firm improves their Security Monitoring by subscribing to 24x7 Information Security surveillance.**

### ***The Challenge***

India's Reputed Financial firm has around 1000 users spread across Indian Territory divided into Primary, Disaster Recovery, Tier-1 locations with leased line connectivity, Tier-2 locations with internet IPSEC VPN connectivity, Tier-3 location with Broadband IPSEC VPN connectivity. Their corporate office is setup in Nariman Point as Primary Datacenter & Andheri as their Disaster Recovery center. Their IT setup hosted multiple applications including Microsoft Domain, MS Exchange Mail messaging solution, Blackberry Enterprise Services, Financial Applications etc. Since the IT operations ran 8x5 proper insight into network activity was not done on a real-time basis, Customer needed round the clock monitoring of their security posture along with Weekly reports. Customer introduced ADSL to provide appropriate solution. ADSL introduces 24x7 Information Security Surveillance Service to the Customer to further improve their security posture.

### ***Our Approach***

Allied Digital Network & Security Consultants conducted a detailed study of their network and security infrastructure and suggested the proper topology in terms of securing their identity and maintaining high level of Confidentiality, Integrity & Availability for Information assets. Allied Digital conducted a detailed Gap analysis through network & security audit to clearly identify the Vulnerability in the existing network infrastructure. ADSL team conducted Vulnerability Assessment on their perimeter security devices and rectified the policy vulnerabilities and configuration errors ADSL team redesigned their perimeter security strategy from single tier to two tier design. Identification of critical Business critical segment was done and best of the class Intrusion Prevention was deployed for deep insight into packet payload flowing in & out of these critical systems. Logs from Perimeter Security devices & IPS were forwarded to Event Manager for event correlation between various security devices.

ADSL SOC consultants deployed e-Cop Event Manager (SOC component) in the Primary and Disaster Recovery Center to capture the Real-time security events from security devices deployed at strategic location. These security events were normalized and sent to ADSL SOC in a secured manner where ADSL security Analyst monitored the events in real-time 24x7. In case of any intrusion or Passive attack detected on the Monitoring System, a disruption module would be activated in the Monitoring system resulting in shunning the malicious source through time based ACL deployed on the specific security devices from where the intrusion is detected. ADSL also suggested web content filtering, Email security, Asset Management & Endpoint security to provide additional layer of defense for the end user computing, which would prevent intrusion of malicious .Allied Digital did the integration in a phased manner with zero downtime to the users in corporate office. After successful completion, company signed long term service contract with Allied Digital to support their mission critical corporate network at all India location.

### ***Results***

Financial Company has seen significant improvements in their network security posture after opting for 24x7 Information Security Surveillance Service. Early Detection and Remediation is also achieved reducing the risk in intrusion attempt during non monitored hour. Company appreciated the solution and services provided by Allied Digital & engaged ADSL for all India level Infrastructure management service.

### ***Solution Building Blocks***

- Cisco ASA Perimeter Security solution.
- Checkpoint + Nokia Perimeter Security solution.
- Real Secure ISS IPS.
- Websense Web Content Security.
- Postini Email Security.
- e-Cop Security Incident Management.
- Qualysguard Vulnerability Assessment.
- LANDesk Management Suite & Security Suite 8.8
-

***Services Offered by Allied Digital in this project***

- Project Consultancy
- Network & Security Audit
- Project Management
- Security Incident Management.
- Annual Maintenance Services
- Infrastructure Management Services