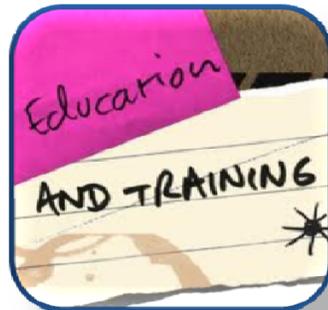# MIEL e-Security Pvt. Ltd.

One-stop-shop for Information Security Services

The Group

Information Security Space - an Introduction

MIEL Summary

MIEL Offerings

MIEL Clients

The Group

MIEL

- Information Security Services, Training and Solutions Company

STB Technology

- Operates in EMEA and ASIA Pacific
- Business-Technology Consulting
- SAP, EPM
- Security
- Cloud Offerings
- Listed on Bombay Stock Exchange

Introduction to Information Security Space

Information Assets

Printed or written on paper

Stored electronically

Transmitted by mail or electronic means

Shown on corporate videos

Spoken in conversations

Classified Information

- ✓ Intellectual Property
- ✓ Business Plans
- ✓ Customer Details
- ✓ Financial Records
- ✓ Future Plans

Safe – As long as it stays where it should be!

Locations

- » On the hard disks of
  - Servers
  - Desktops
  - Notebooks
- » In back up media
  - Tapes / CDs
  - DATs
- » Documents
  - Reports
  - Forms
- » Internet Web Servers
- » E- mail inbox
- » Trash cans: physical & logical
- » Employees
- » Contractors / Service Providers
- » Trainees
- » Consultants
- » Customers
- » Associates

Threats

- » Physical Theft
  - Theft of devices
  - Theft of media
- » Logical Theft
  - Illegal copying
  - Stealing password
  - Hacking
  - Trojan
  - Espionage
- » Digital Mess
  - Uncontrolled Versions
  - Orphaned Data
- » Social Engineering
- » Data Corruption
  - Virus attack
  - Information modification
  - Forgery
  - Sabotage
  - Fraud
- » Data Denial
  - Denial of service
  - Business continuity risk

MIEL Summary

Information Security Pioneer in India

One of the largest Pure-play Standalone Info-sec Company in India

Experienced Professionals

Partnerships: Academic (10), Business (36)

Values, Business Model

Brand

IPs/IPRs

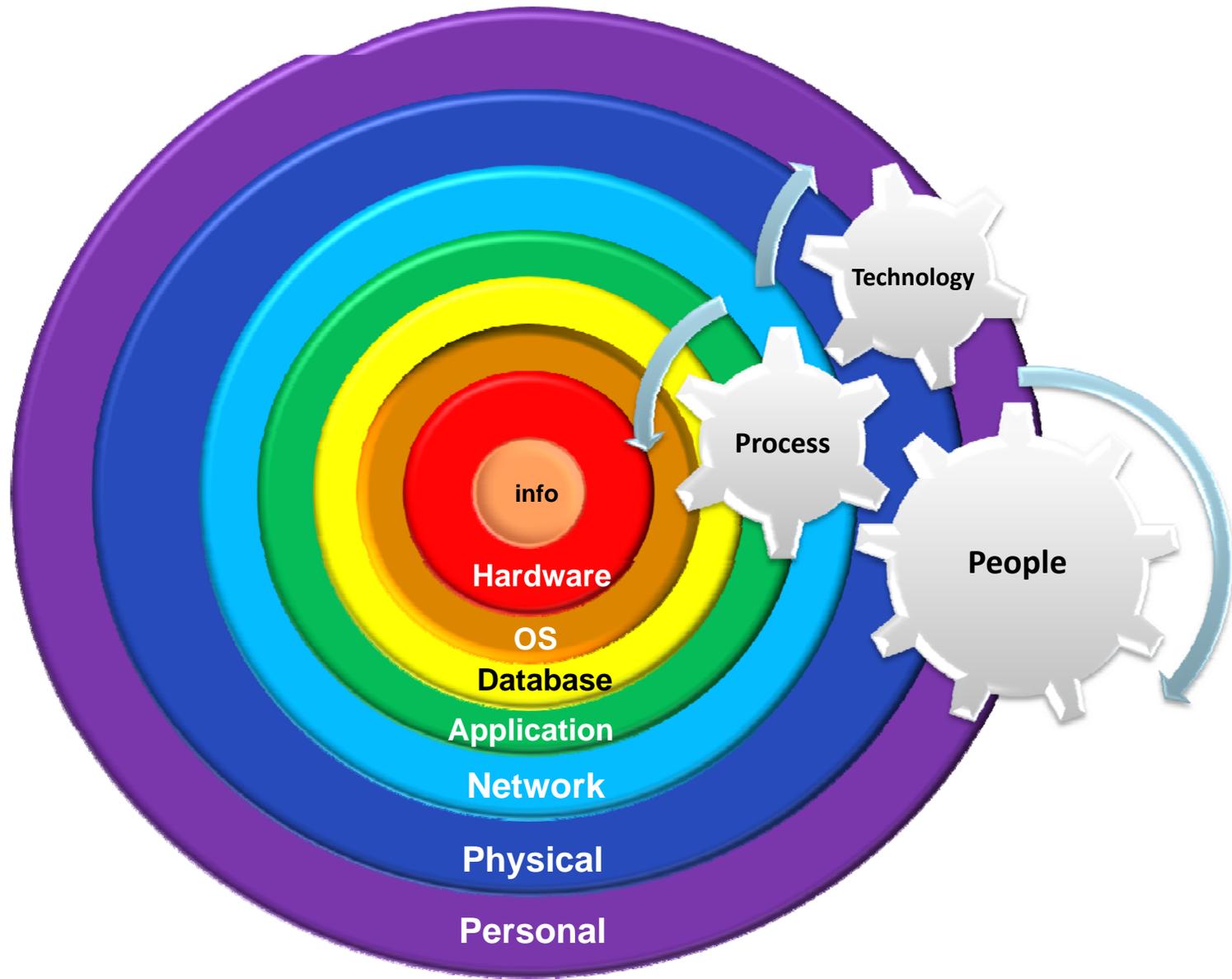One-of its kind Info-sec Education Services Company

Clients and Global Footprints
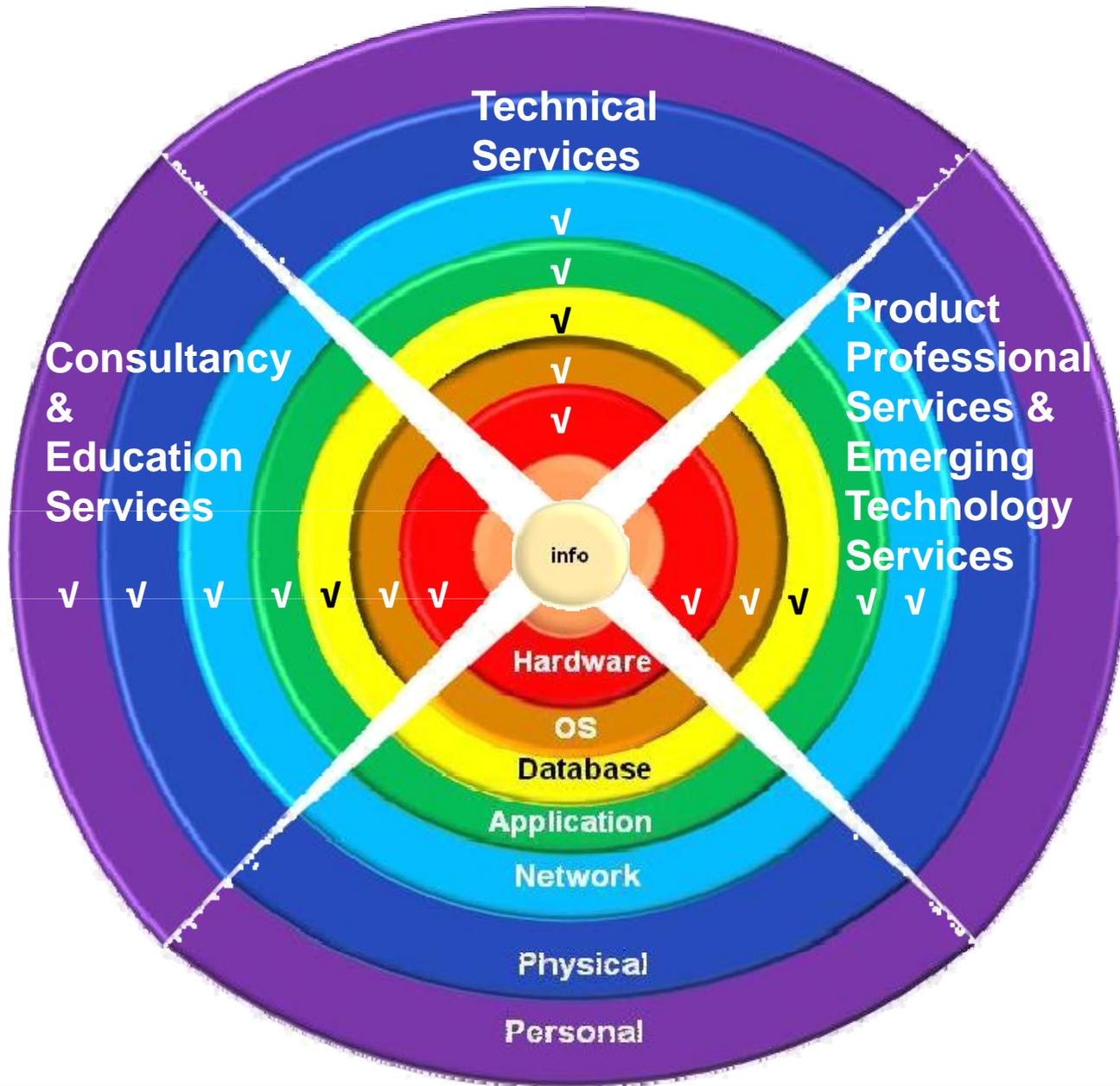
Accolades & Testimonials

Potentials of Each Division, Ramp-up Capabilities

EL's Holistic Approach to Information Security

MIEL Services

Technical Services

√
√
√
√
√

Consultancy & Education Services

Product Professional Services & Emerging Technology Services

√ √ √ √ **√** √ √   √ √ **√** √ √

info

Hardware

OS

Database

Application

Network

Physical

Personal

MIEL Offerings

Services

NSULTANCY SERVICES
organizational compliance with IS standards like
27001, BS 25999, PCI DSS, HIPAA, Data Privacy, etc.

CHNICAL SERVICES
ervices like penetration testing, vulnerability
essment, application security and forensics etc.

NAGED SECURITY SERVICES
- MIEL End Point Diagnostic Service
- Network Penetration Test, Application Test etc
- Security Operations Center (SOC) for remote
  managed services
- n-source and out-sourced MSS

ODUCT PROFESSIONAL SERVICES
igning, Implementing and supporting technology
tions in partnerships with leading global IS vendors

ERGING TECHNOLOGIES SERVICES
vices in emerging technologies including Data Leak
vention (DLP), IRM, SIEM, PIM, Embedded
urity, Application Control, Integrated on-premise /
d Identify Management & SSO

IPs

- **Helios Platform**: Agent-less technology allowing the client to centrally audit security levels on the desktops and servers in the organization

- **Risk Metrics**: Provides the client a dashboard on the level and trend of security parameters

- **3nigma:** Provide assurance Software Licensing Compliance

Education & Training

LONG TERM COURSES
Programme in Information Security (PRISM):
One year Post Graduate programme for
specialization in IS Management

SHORT TERM COURSES
Information Security Training Institute (ISTI):
Instructor led training

END-USER TRAINING covering End-Users in
Corporates, Government etc

PUBLIC AWARENESS PROGRAMS
New high-growth initiatives to address the
largely untapped non-enterprise, mass market
segments like schools, colleges etc

KNOWLEDGE PROCESS OUTSOURCING (KPO)
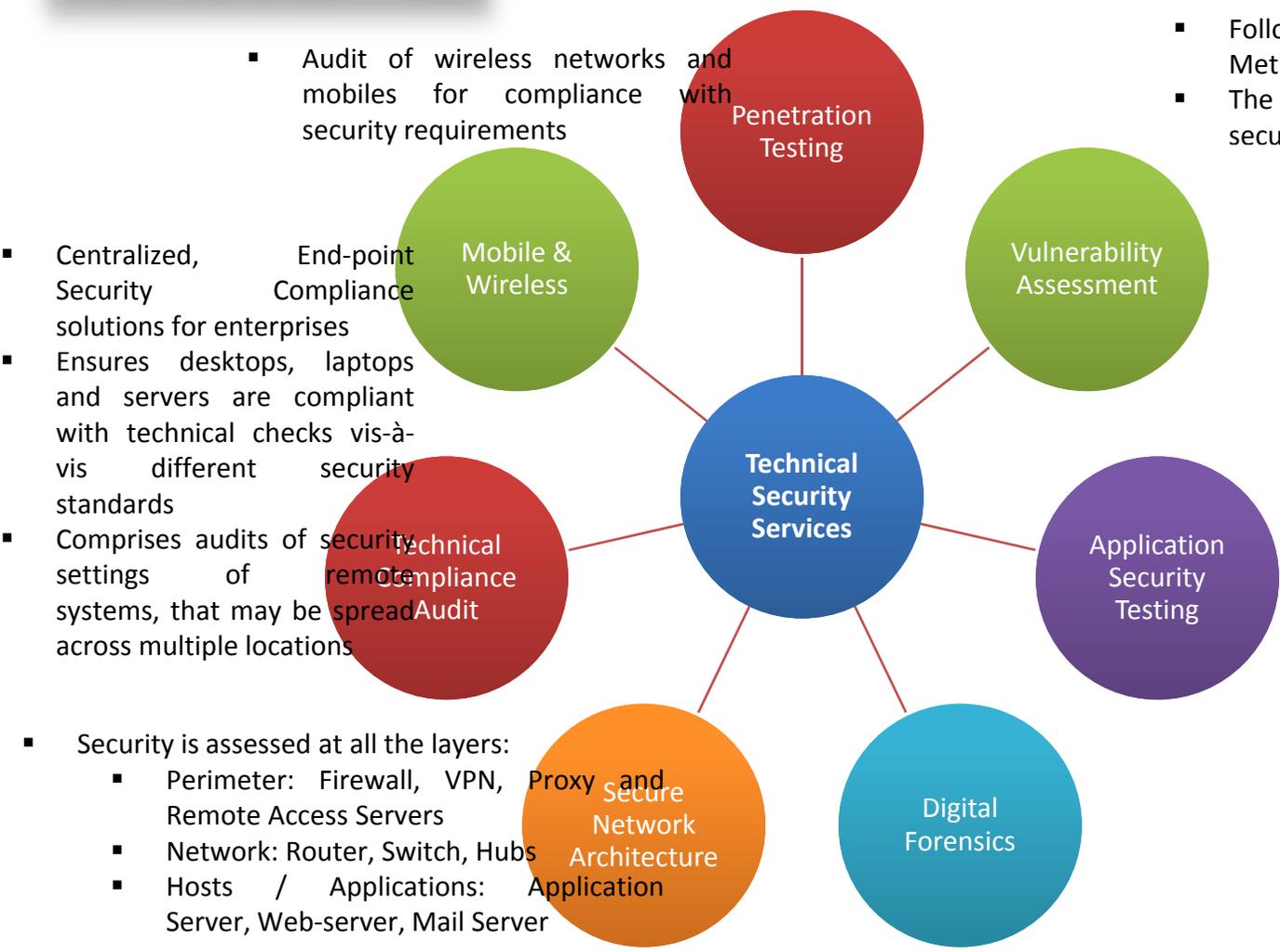Developing Course Content for global IS
education majors

CONSULTANCY SERVICES

- Company provides consultancy to Organizations on complying with various Information Security standards like ISO 27001, BS 25999, ISMS, BCMS, PCI DSS, CoBIT, HIPAA etc.
- Besides the above listed standards, MIEL also provides consultancy services for compliance with other security audits- ATM audits, Branch audits, Risk mitigation and assessment etc.

Standard/ Framework	Governing Principle
ISO 27001	▪ ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control
ISMS (Information Security Management System)	▪ An organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets
BCMS (Business Continuity Management System)	▪ Based on ISO 22301, BCMS provides a management framework that gives organization the necessary controls to address risks and monitor and measure their ability to manage, and recover from, disruptions
PCI DSS (Payment Card Industry Data Security Standard)	▪ Information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
CoBIT (Control Objectives for Information and Related Technologies)	▪ Framework created by ISACA for IT management and IT Governance ▪ Allows managers to bridge the gap between control requirements, technical issues and business risks

Phase I Information Security Profiling → **Phase II** Information Security Prescription → **Phase III** Information Security Treatment → **Phase IV** Information Security Vigil → **Phase V** ISO 27001 Certification

HNICAL SERVICES

- Audit of wireless networks and mobiles for compliance with security requirements

- Centralized, End-point Security Compliance solutions for enterprises
- Ensures desktops, laptops and servers are compliant with technical checks vis-à-vis different security standards
- Comprises audits of security settings of remote systems, that may be spread across multiple locations

- Security is assessed at all the layers:
  - Perimeter: Firewall, VPN, Proxy and Remote Access Servers
  - Network: Router, Switch, Hubs
  - Hosts / Applications: Application Server, Web-server, Mail Server

Penetration Testing

Mobile & Wireless

Vulnerability Assessment

Technical Security Services

Technical Compliance Audit

Application Security Testing

Secure Network Architecture

Digital Forensics

- Follows the OSSTMM (Open-Source Security Testi Methodology Manual) standards
- The OSSTMM is a peer-reviewed methodology for performi security tests and metrics

- The Assessment involves the security of Information S as an internal attacker, referred to as ethical hacker

  - Black-box testing
  - Grey-box testing
  - White-box testing
  - Grey-box testing & se code-review

- Audit user activities
- Expert witness services
- Consultancy Services
- Computer Forensics

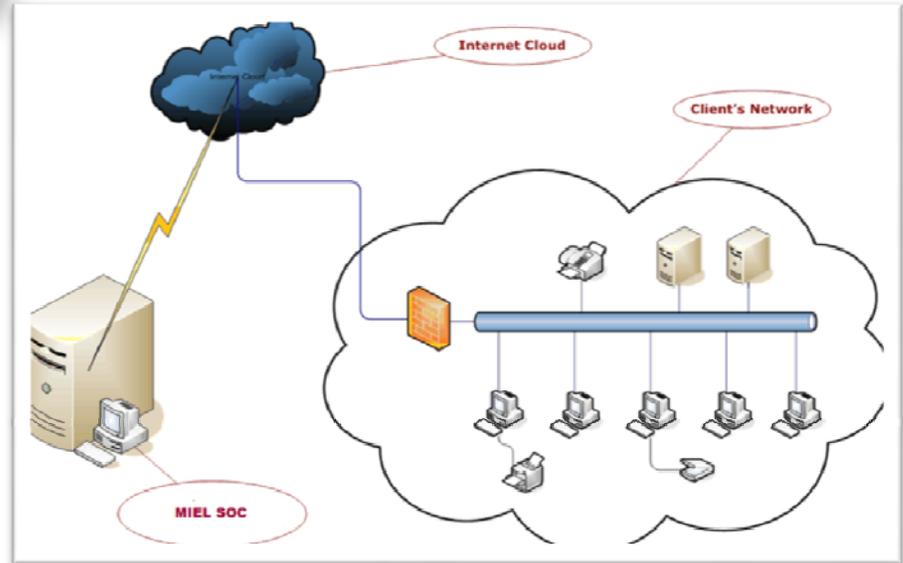## NAGED SERVICES (IN-SOURCED MODEL)

Daily Activities	Weekly Activities	Monthly Activities	Quarterly Activities	Half-yearly Activities
▪ Firewall Administration ▪ User Registration/de-activation ▪ Server Log Analysis, ▪ Virus, Worms, malware advice ▪ Monitoring for central virus updates ▪ Desktop Audit ▪ Compliance Review	▪ OS, configuration and application backup review ▪ Off-site backup media movement ▪ Restoration test ▪ Cracking weak and default passwords ▪ Compliance Monitoring	▪ Server room access verification ▪ Latest upgrades verification ▪ Application access matrix verification ▪ Program change control ▪ Version Control ▪ Compliance ▪ Status Report on security to ISSM/ISD	▪ VA, Manual Review and Hardening of OS,DBMS, Web-server ▪ Review of Network architecture and Recommendations ▪ Environment and Physical Security ▪ DRP review ▪ Compliance Monitoring	▪ Half-yearly audit

Underlying Devices and Systems

▪ Firewall ▪ Content Filter ▪ Anti-virus Servers ▪ Desktops	▪ Backup Media and documentation ▪ Password Crack	▪ Physical Security Devices ▪ Servers ▪ Program/Version control documents	▪ Servers/OS ▪ DBMS ▪ Server Room ▪ DRP document	▪ All systems and documents

NAGED SERVICES (REMOTE MODEL)

Security Device Life Cycle Management Services

- Management of Security devices
- Minor Patch Implementation
- Vendor Support Services
- OEM Support Services

Vulnerability Management

- Remote Tools Based Scanning for Vulnerabilities
- Remote Patch Management for Mitigation of Vulnerabilities

Security Incident And Event Monitoring Services

- Near Real Time Monitoring of Logs from Devices
- Alerting for Security Incidents using Correlation Techniques

- **Delivery From MIEL SOC**
- **Shared Resources and Tools**
- **Service window**
- **SLAs as per Agreement/ Contract**

RODUCT PROFESSIONAL SERVICES

MIEL has partnered with the "best-of-breed" technology vendors to implement IS solutions or clients and have built high-end skill sets and track record of large scale implementations

Knowledge transfer and training of the client's employees
Technical support services

Enterprise Storage audit
Backup and Restore software audit
Data-center audit
BCP/ DR audit

Project Assessment

Training and Support

Security and Availability

Planning & Design

Audit Services

Project Implementation

- Review current environment and examine business and technical issues
- Perform problem definition and document objectives
- Prepare Proof-of-Concept if desired

- Understand existing architecture a technical direction
- Formulate an integration strategy th leverages existing proven host application business rules and data
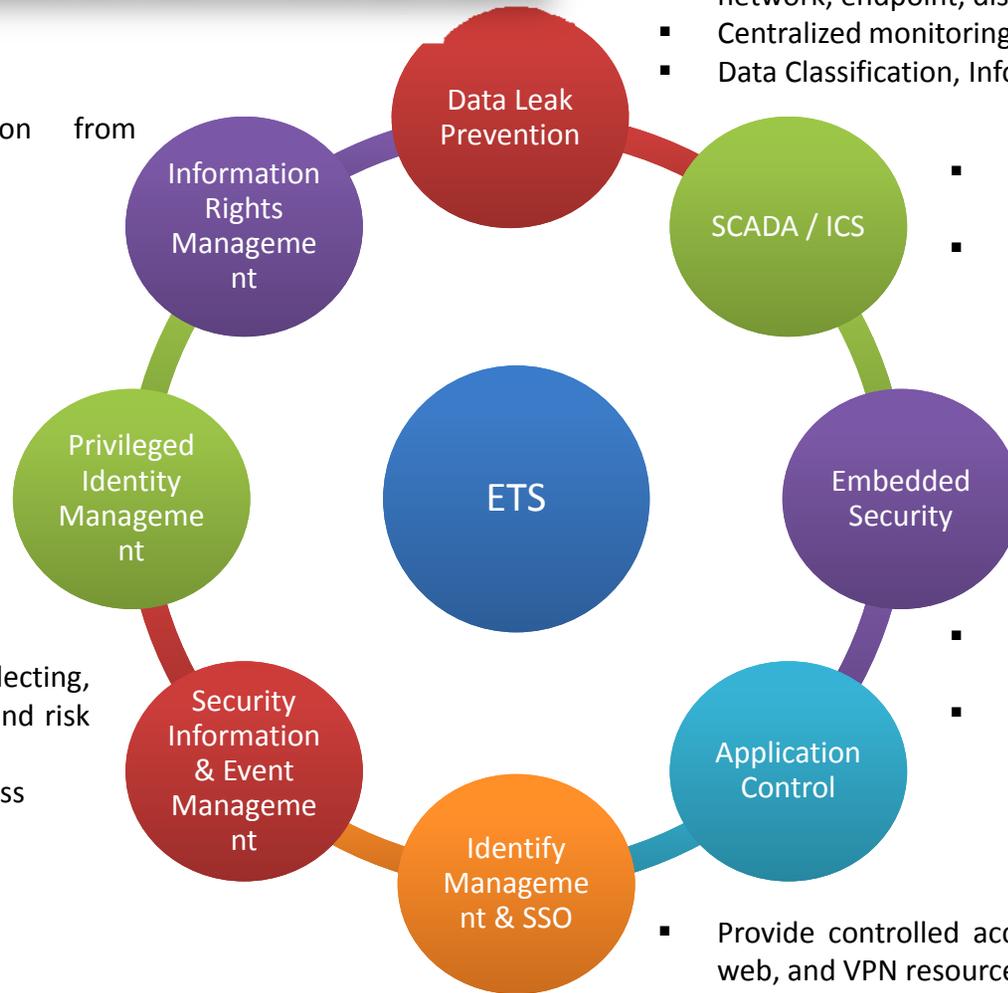- Prepare a solution design that is scalab keeping in view future requirement

- Installation and configuration of the software/hardware
- Perform User Acceptance testing as per the plan
- Operational administration orientation
- Project Sign-off

GING TECHNOLOGY SERVICES (ETS)

- Automated real-time enforcement options across network, endpoint, discovered data repositories
- Centralized monitoring and reporting
- Data Classification, Information Identification, Risk Assessment

- Prevent sensitive information from unauthorized access
- Dynamically control data usage

- SCADA / ICS: Cyber security threats vulnerability assessment
- Advanced SCADA cyber security training

- Provide controlled access to privileged accounts based on security policies
- Provide granular control to the commands super-users can run

- Secure embedded devices
- Automate the enforcement of software change control policies on them

Diagram (circular):

Center: **ETS**

Surrounding nodes:
- Data Leak Prevention
- SCADA / ICS
- Information Rights Management
- Embedded Security
- Privileged Identity Management
- Application Control
- Security Information & Event Management
- Identify Management & SSO

Integrated product platform for collecting, processing and assessing security and risk event info
Training for SIEM product and process

- Protect against zero-day and advance persistent threats without signature updates
- Enforce controls on connected disconnected servers, virtu machines, endpoints, fixed devices

- Provide controlled access and user management services for eve web, and VPN resource
- Automatic infrastructure integration on and/or off-premise

Product Solutions

Security Offerings

Anti-Virus Encryption |Mobile Security | Proxy, Load Balancing | Web Security |
2 Factor Authentication | Email Security | Firewall | DLP

Storage Offerings

Backup & Recovery Services | High Availability | Optimization
Support Services | Information Infrastructure Management
Audit Services | Archival & ILM | Enterprise Storage Strategy
Product Consulting

os / Endpoint Diagnostic Services

y Benefits:

Check 200 security parameters on your desktops & servers...

For standards like ISO27001, PCI/DSS, SOX, HIPAA, GLB, NIST etc...

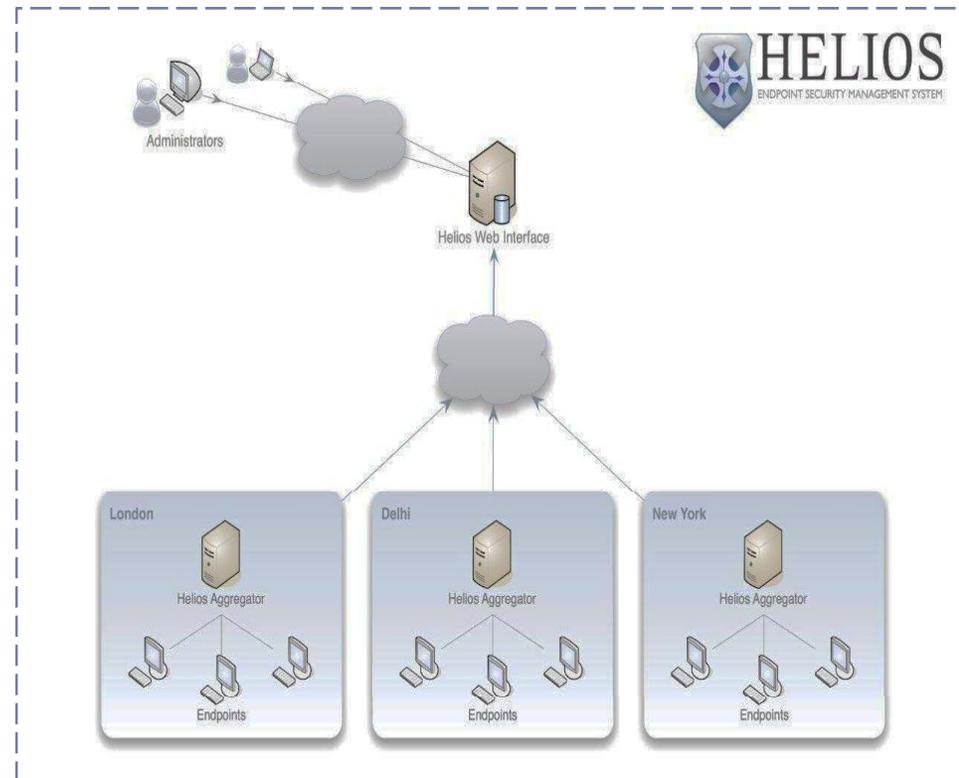Without installing any agent software or making network modifications...

Regardless of the number of desktops & servers...

Across any geography...

With customized reporting, checks and trend-analysis...

On demand, or on a regular schedule...

At a compelling price.

Accolades/ Awards

- Nominated for NASSCOM IT Innovation Awards
- Recognition at Black Hat Conference held in Las Vegas
- Used as a case study for anti root-kit technology at the Georgia-Tech University

Powered by **MIEL HELIOS** ™
ENDPOINT SECURITY MANAGEMENT SYSTEM

Some Common Compliance
Questions That Helios Answers…

Leveraging MIEL's in-depth knowledge of how audits are conducted, we built Helios to answer questions that your auditors are sure to ask. Here are just a few examples…

**Helios / Endpoint Diagnostic Service c
answer and report on 200 similar que
out of the box**

- ☑ Is an anti-virus installed, is it updated and is the auto-protect enabled?

- ☑ Are automatic updates being downloaded or installed?

- ☑ What network shares are on the system?

- ☑ What software is installed on the system and what versions are they?

- ☑ What programs are running on the system right now?

- ☑ Is the desktop firewall enabled and what applications/ports are allowed?

- ☑ Who are all the users on the system?

- ☑ Which users are local administrators, and is the current user an administrator?

- ☑ What logging is enabled on the system?

- ☑ What length of passwords are accepted?

- ☑ What services are installed?

- ☑ Does the system display confidentiality/ unauthorized access prohibited messages before users login?

- ☑ Does the system automatically login without a password?

- ☑ What Windows hot-fixes/ patches are installed?

- ☑ Is registry editing disabled?

- ☑ Do accounts lock-out after a number of incorrect passwords?

- ☑ For how long do accounts lock-out?

- ☑ How many passwords are remembered for password history?

- ☑ Does the screensaver lock prevent unauthorized users from using the system?

- ☑ Can USB devices be connected and on what dates were they written to?

- ☑ Is the guest account disabled?

- ☑ Who can change advanced browser settings?

- ☑ What sort of network encryption does the system perform?

- ☑ Does the system use strong encryption algorithms for passwords?

- ☑ Which users have rights over key system functions such as installing hardware?

Helios can answer close to 200 similar questions right out of the box.

OTHER INFORMATION SECURITY – IPs

▸ **Risk Metrics**

- ▸ Risk Metrics provides a Top Management Information Security Dashboard for a review of the status of several of the IS parameters across the organization

- ▸ It helps senior business management realize priority areas, with drill-down to basic data

- ▸ The first version was built for one of the largest private sector banks in India

▸ **3nigma**

- ▸ This product idea germinated through Consultancy practice, and taken shape as a tool covering Software classification

- ▸ The product is expected to facilitate projects where clients would assurance on the level of their Software Licensing Compliance

▸ **Risk Metrics Sample Dashboard**

Awareness	Asset Management	Desktop Compliance	Data Protection	Malware Management
Security Monitoring	Risk Management	Security Incident Management	E Commerce	Identity & Access Management
Application Security	Governance	Policy	Change Management	Business Continuity Management
	Accountability & Ownership	System Configuration	Privacy	

MIEL Academy

Short-term Courses (ISTI) : 1-5 days

Long-term Courses (PRISM + Eklavya)

End User Training Awareness

Knowledge Process Outsourcing

Certification Courses

MIEL Courses

1 Year Program

2 - 4 Hours e-Learning Program

Global Course Content Development

Program in Information Security Management (PRISM)
Coverage

Orientation	Trimester 1	Trimester 2	Trimester 3	Trimester 4
• Computer Fundamentals • Introduction to Networking • Basics of C • RDBMS Concepts and SQL Basics • Basics of PLSQL Programming • Basics of Java Programming	• Information Security Introduction • Physical and Environmental Security • Access Control • Cryptography Fundamentals • UNIX Architecture • Web Application Security • Network Security	• Operations Security • UNIX and LINUX Security • Windows Architecture • Wireless Communications and Telephony • Applied Cryptography • Computer Audit and Assurance • Cyber Crime Investigations and Forensics	• Database Security • Windows Security • Security Models, Frameworks and Guidelines • Security Certifications • Security Incident Management • Business Continuity & Disaster Recovery	• Cyber Laws & Anti Money Laundering • Enterprise Security Architecture • Cloud Computing & Virtualization • Project Work

End-User Security Awareness Training
Solution

Features

- Training Need Analysis
- e-security training Content
- Quiz/Test per module
- Content/Course Management
- Import/Embed files
  (PDFs, Audio, Video etc.)
- Assignments
- Employee Activity Tracking
- Glossary
- Discussion Forum
- Real-time Chat
- Interactive Games
- Announcements/Alerts
- Result Management
- Reporting
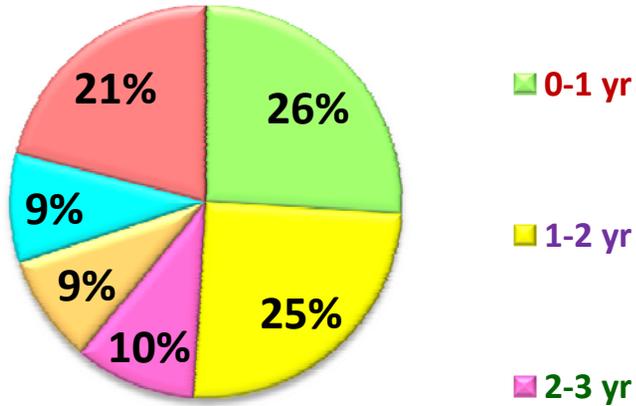- Look & Feel Customization
- End-to-end Support

Modules

- Password security
- Social Engineering
- Social Network security
- Email security
- Physical security
- Phishing
- Anti-virus and Malware
- Instant Messenger Security
- Wireless security
- Mobile devices security
- Browser security
- Controls against Hacking
- Insider threat
- Secure computer operations
- Organization's Information
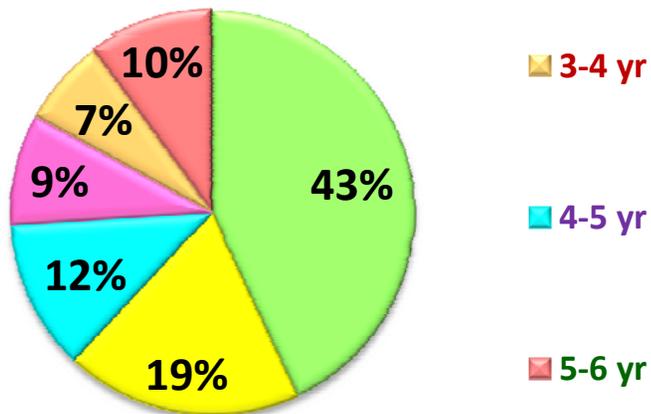 Security Policy awareness

FY 12 Clients Revenue

- 21%
- 26%
- 9%
- 25%
- 9%
- 10%

FY 12 Clients Count

- 10%
- 43%
- 7%
- 9%
- 12%
- 19%

Legend:
- 0-1 yr
- 1-2 yr
- 2-3 yr
- 3-4 yr
- 4-5 yr
- 5-6 yr

- Top 10 clients accounted for 32.4% of the overall business in FY12

- Average tenure of relationship with Top 10 clients is 3 years

- Overall 38% of the clients have been with MIEL for last 2 years and more, and account for 49% of the total business

- Being a high quality service provider in the niche space, the company is the first name to be recalled for security projects for its clients

MIEL: Select Clients

BFSI

MEDIA/ENTERTAINMENT/PHARMACEUTICAL/TRAVEL/MANUFACTURING

INTERNATIONAL

IT / ITeS

Others

Track Record

Middle East

Sri Lanka

Africa & South East Asia

Thank You

Nitin Umesh (Group Chairman & Founder)

Email :

nitin@stbtechnology.com

Info@stbtechnology.com

Website :

www.stbtechnology.com