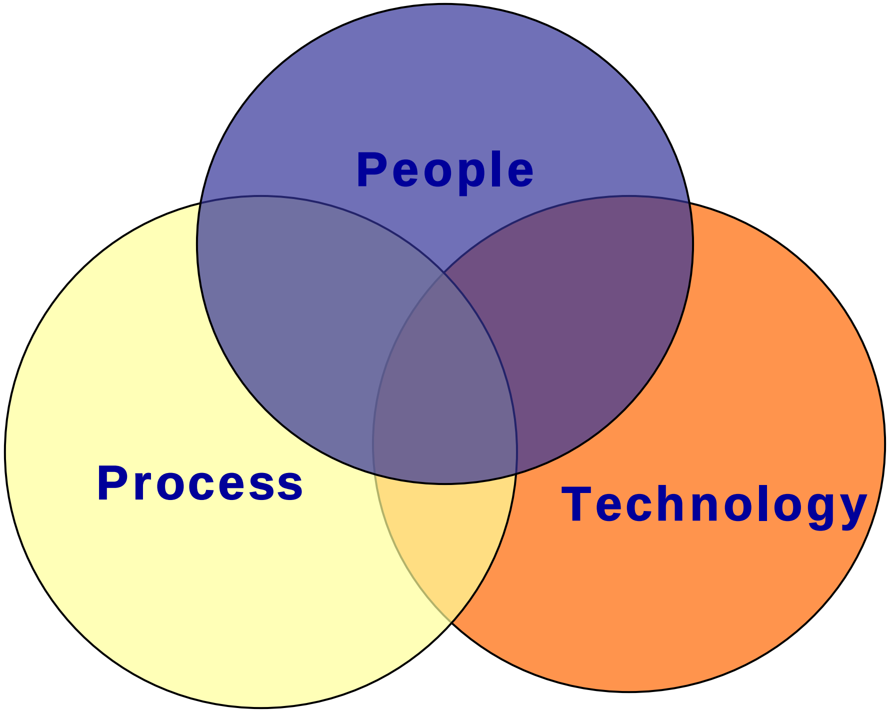
NUS InfoComm Security Landscape

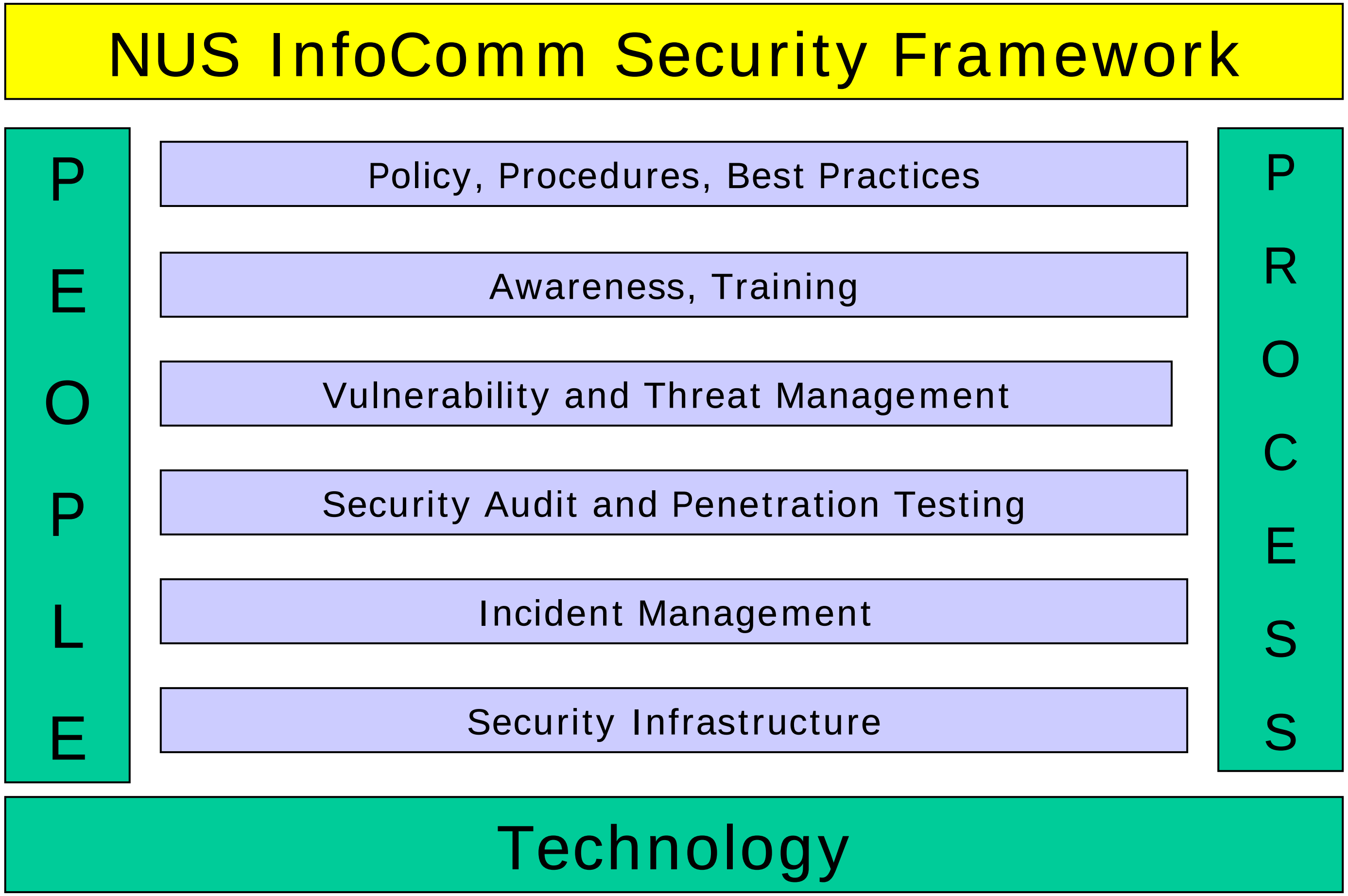
Yong Fong Lian,
Manager (IT Security), NUSCERT,
NUS, Computer Centre

NUS
National University
of Singapore

NUS Security Strategy



NUS Security Framework



NUS InfoComm Security Framework

PEOPLE

Policy, Procedures, Best Practices

Awareness, Training

Vulnerability and Threat Management

Security Audit and Penetration Testing

Incident Management

Security Infrastructure

PROCESS

Technology

People : Policies, Procedures, Best Practices

- Policies, Standards, Control Procedures
  - NUS IT Security Policy
  - Acceptable Use Policy
  - ISO 27000 compliant policy
  - ISO 9001:2000 certified procedures
  - Portals facilitate secure access to policies

- Best practices
  - US-CERT
  - SingCERT
  - SANS

People: Awareness, Training

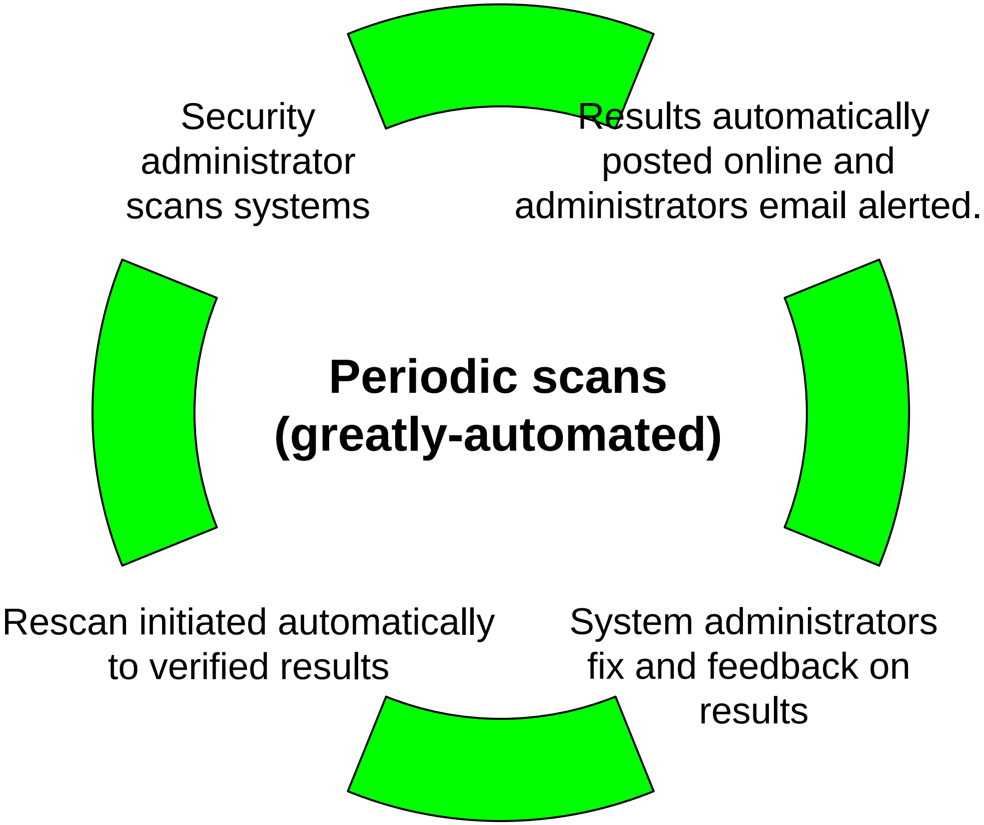
- Awareness
  - NUS IT Security Week
  - Freshman Security Orientation Week
  - IT Security e-Newsletter, Blog
  - Email, MOTD alerts, SMS alerts
- Training
  - Online Security Module (staff and students)
  - End User Security Training (admin staff)
  - Technical Security training on Firewall, IDS, Windows, Linux, Apache, Application Security Controls
  - Certification Program (systems and network administrators)
  - Systems Accreditation Program

Process: Vulnerability Management

- Vulnerability management
  - Network Address Tracking and Security (NATS)
  - Scans from Internet and within NUSNET
  - Quarterly scans for mission critical servers
  - Campus wide scans (full scans and incremental scans)
  - Vulnerability self-assessment (ad-hoc scans)
  - Multiple scanners for cross-checks
  - In-house web-based portals and systems with workflow
  - Vulnerabilities evaluated at system, network, application and database levels
  - Automated patch management for Windows
  - Auditing of Disk Images before deployment

Vulnerability and Threat Management (Process)

Campus wide scans



Security administrator scans systems

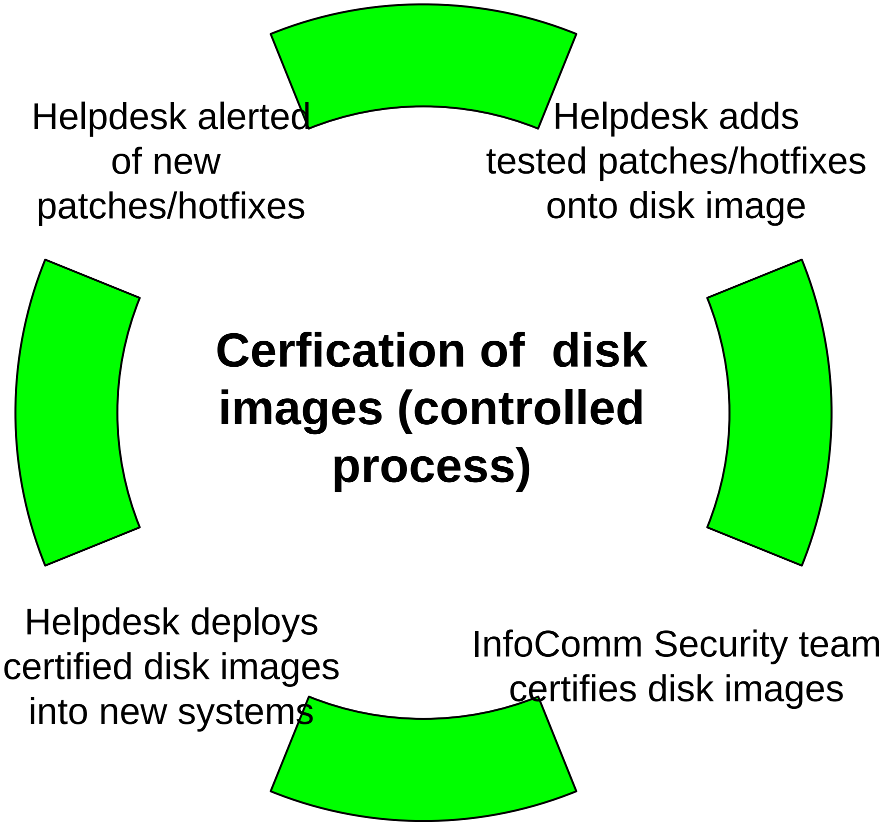
Results automatically posted online and administrators email alerted.

System administrators fix and feedback on results

Rescan initiated automatically to verified results

Periodic scans (greatly-automated)

Certification of disk images



Helpdesk alerted of new patches/hotfixes

Helpdesk adds tested patches/hotfixes onto disk image

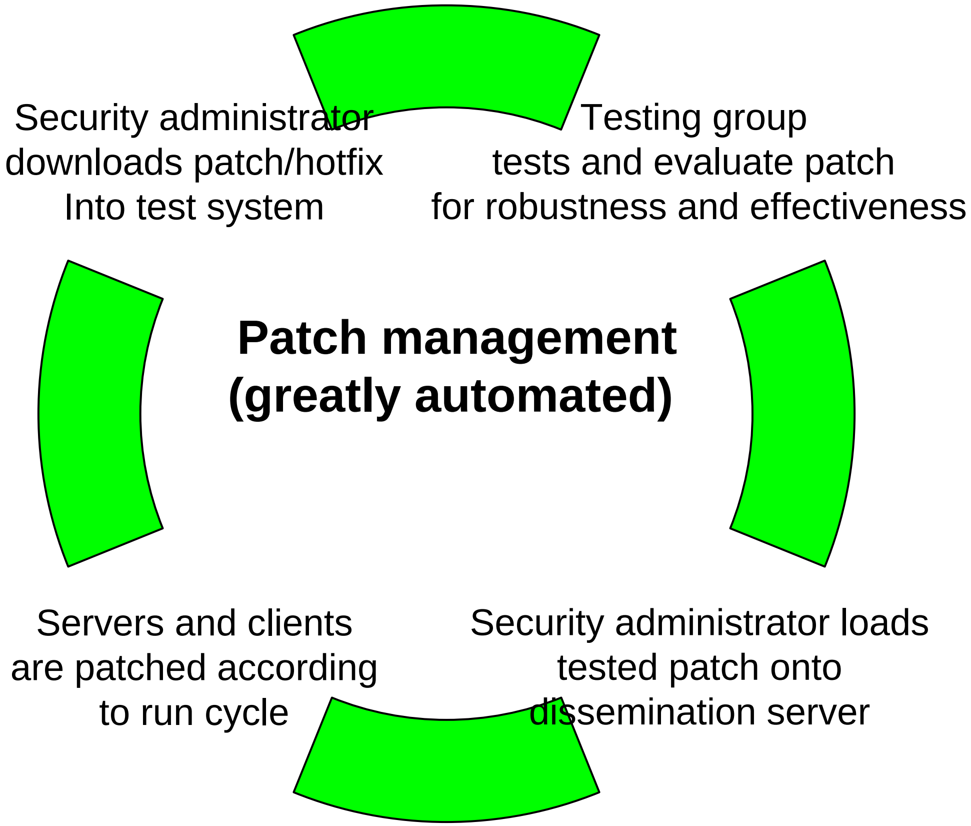
Cerfication of disk images (controlled process)

InfoComm Security team certifies disk images

Helpdesk deploys certified disk images into new systems

Vulnerability and Threat Management (Process)

Automated patch management



Security administrator
downloads patch/hotfix
Into test system

Testing group
tests and evaluate patch
for robustness and effectiveness

Patch management
(greatly automated)

Security administrator loads
tested patch onto
dissemination server

Servers and clients
are patched according
to run cycle

Process: Threat Management

- Threat management
  - SANS Top 20 vulnerabilities Editing Comm
  - In-house Vulnerability Alert System
    - Alerts include SANS, SECUNIA, Microsoft, BugTraq, SecurityTracker.
    - Allows user subscription to relevant ones
  - Mechanism of alerts
    - Email and SMS
  - Threats are assessed and mitigated
    - patch management
    - updates to firewall rules
    - blocking attachments at email gateways
    - blocking outbound access to malicious sites at proxy

Process : Security Audit, Penetration Test

- Security audit (internal and external periodically)
  - Audit on policy compliance
  - Audit on technical control compliance
  - ISO 9001 audit on security processes
  - Audit of disk images before deployment
- Penetration test
  - Social engineering penetration test
  - Password audits
  - Technical penetration test
    - System, network (e.g. firewall), database, application
  - From Internet and within NUS network

Process : Incident Management

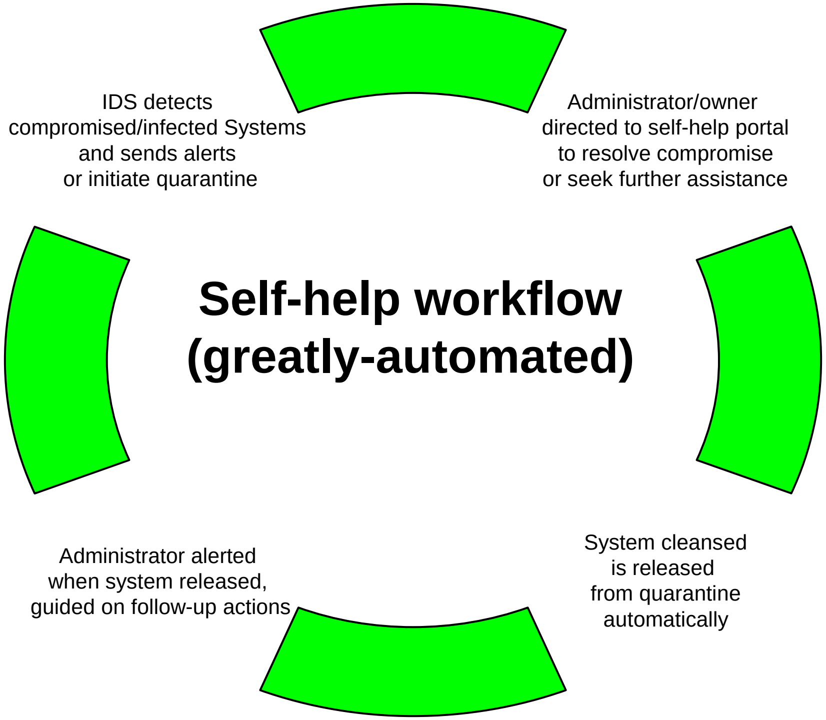
- Incident management and Forensics
  - Existing threats
    - Signature-based IDS
    - Behavioral-based IDS
    - Honeynet
    - Detection at network and host levels
    - SANS advisory
    - FIRST advisory
  - Compromised or infected systems are quarantined and redirected to a self-help page for remedy
  - Detection of new virus via scanning of attachments at the email gateway with multiple virus scanners

Process : Incident Management

- Incidents include systems compromises, email misuses, copyright infringement, virus etc.
- Follows standard incident management guidelines
- CERT/CC and SANS recommended incident handling tools are used in manual investigations.
- Owners of compromised/infected systems are automatically alerted or quarantined for remedial actions in a self-help workflow.

Process : Incident Management

- Self-help workflow



Self-help workflow (greatly-automated)

IDS detects
compromised/infected Systems
and sends alerts
or initiate quarantine

Administrator/owner
directed to self-help portal
to resolve compromise
or seek further assistance

System cleansed
is released
from quarantine
automatically

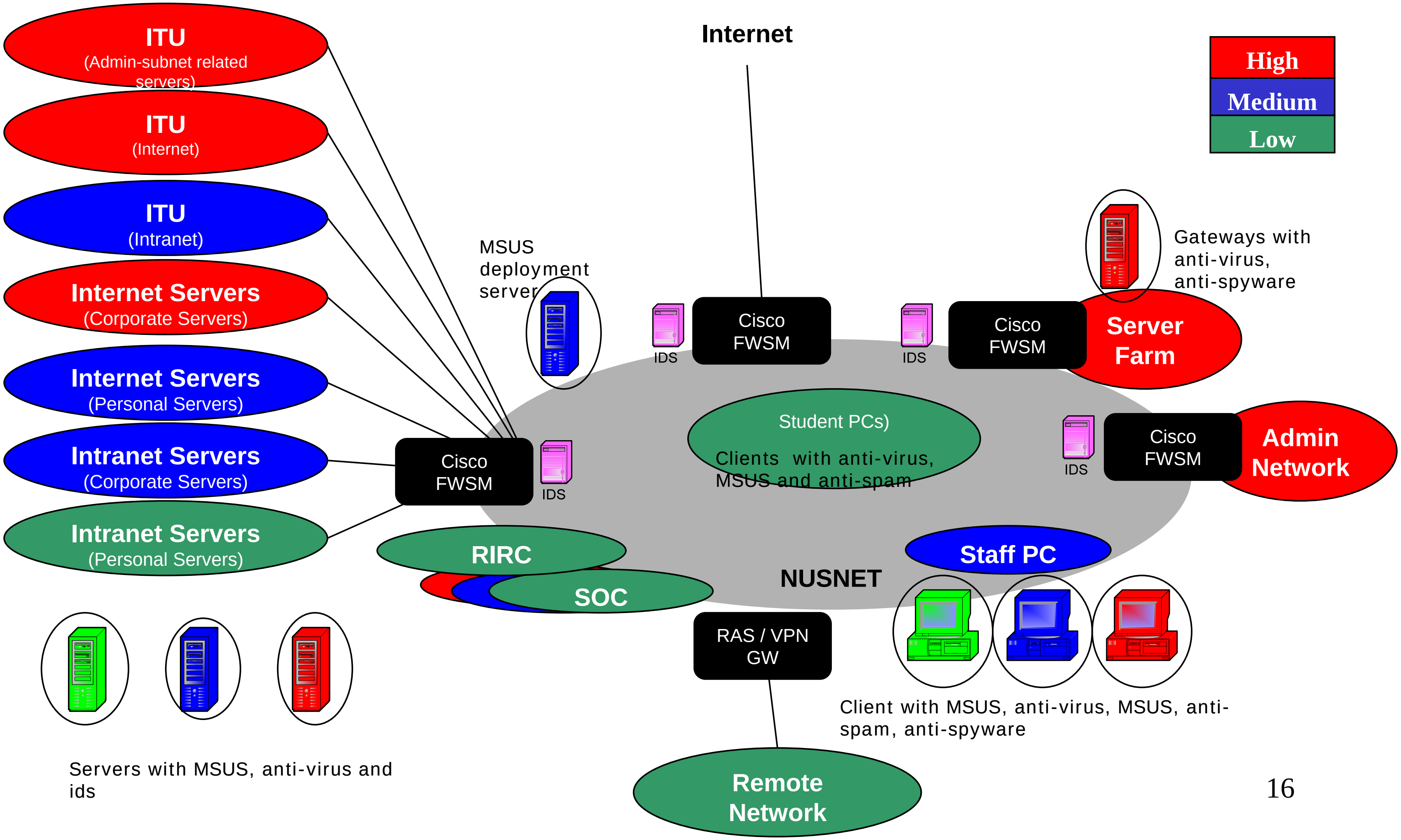
Administrator alerted
when system released,
guided on follow-up actions

Technology : Defence in Depth Infrastructure

- Segmentation of network into different levels of security
- VPN used to encrypt sensitive data transmitted across network
- Firewalls, IDS, anti-virus, anti-spyware, anti-spam installed at server and client

	Gateway	Server	Client
Firewalls	√	√	√
IDSes	√	√	√
Anti-virus	√	√	√
Anti-spyware	√	√	√
Anti-spam	√		√

Technology : Defence in Depth Infrastructure



Internet

High
Medium
Low

ITU (Admin-subnet related servers)

ITU (Internet)

ITU (Intranet)

Internet Servers (Corporate Servers)

Internet Servers (Personal Servers)

Intranet Servers (Corporate Servers)

Intranet Servers (Personal Servers)

MSUS deployment server

Cisco FWSM

IDS

Student PCs)

Clients with anti-virus, MSUS and anti-spam

Gateways with anti-virus, anti-spyware

Server Farm

Admin Network

RIRC

SOC

NUSNET

Staff PC

RAS / VPN GW

Remote Network

Client with MSUS, anti-virus, MSUS, anti-spam, anti-spyware

Servers with MSUS, anti-virus and ids

InfoComm Security Scorecard

- Finalist for MIS Asia 2006 Best IT Security Strategy Award
- Result of IDA government-wide scan on 60+ critical web servers is 0 vulnerabilities
- 0 security incidents on critical servers
- Certified for inclusion in FIRST (Forum of Incident Response Security Teams), an established and renowned International consortium.
- Member of APCERT, which comprises mainly of national level CERTs.
- Security quality processes are ISO 9001 certified
- More than 15 new worms/variants have been reported to antivirus vendor over last 12 months.
- Patches are deployed are up-to-date within 22 hrs.