Proactive Security Management

1. Overview
2. Proactive Security Management: Prevention Portfolio
3. Proactive Security Management: Reaction Portfolio
4. Questions / Answers
Overview
A SMALL STORY
It was once...

Security Organization OK
Security Practices OK
Security Budget OK (but can better do)
Security Projects OK (Protection/Detection) & security integration in the major projects
Security Sensitizing OK

BUT …
A SMALL STORY
It was once…

- Which is my level of protection? KO
- How to justify the investments requests? KO
- How to check the effectiveness of my tools? KO
- Which are the true threats in the middle of all the security events collected? KO
- How to know if at this moment I undergone an attack? KO
- How to treat relevant security incidents? KO
- How to optimize the employment of my security team? KO
TO WANT
Concentration of the efforts
THE RISK: this universal and omnipresent principle raises the question of its “management” in its noblest expression: the POLICY. That which lays down objectives, defines a lawful framework and points out the fundamental principles.

TO BE ABLE
Liberty of action
CAPACITY: this basic concept is declined of the policy and raises the question of the fields of responsibility (in prevention as in reaction and management of crisis), i.e. of the ORGANIZATION. It allots the fields of competences and intervention.

TO KNOW
Economy of the forces
MEASUREMENT: essential tool of the manager, the evaluation of the risk, the stakes, the impacts, the costs is more than ever on the agenda. Because what imports from now on it is the good decision-making, just and balanced. The economy plays an essential part here.

STAKE: IMPLEMENTATION OF CONTROL

A SMALL STORY
It was once...
The Security Challenge

The management of the 7 families of cyber-risks

Security exceeds the single framework of the network
IT Performance Management Maturity Model

Where are you today and where do you want to be?

**Level 1**
- Reactive
  - Chaotic
  - Ad-hoc
  - Document
  - Analyze usage
  - Fight fires
  - Focus on prevention and real-time
  - Move from best effort to enhanced reliability

**Level 2**
- Proactive
  - Integrates management data into a single portal
  - Enhanced real-time analysis
  - Enhanced alert and event management
  - Problem detection is more application aware

**Level 3**
- Service
  - Define services
  - Role of IT as service provider
  - Monitor business experience
  - Enhanced capacity planning
  - Move to virtualized infrastructure with correlated IT and business metrics
  - Measure “real world” usage experience
  - SLA

**Level 4**
- Business Driven
  - Inform on business as well as IT
  - Integrate asset and performance management
  - Optimizing QoS
  - Holistic view
  - Distributed analysis at multiple points
  - Focus on ensuring Revenue
  - Ready for tomorrow

---

Enterprise Management Associates, 2004
## Performance Management Needs of the Enterprise

<table>
<thead>
<tr>
<th></th>
<th>5 years ago</th>
<th>Today</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
<td>Collect the data</td>
<td>Analyze the data</td>
</tr>
<tr>
<td><strong>Functional Priority</strong></td>
<td>How much is the network is used?</td>
<td>How is the network being used?</td>
</tr>
<tr>
<td><strong>Key services</strong></td>
<td>Frame Relay, ATM, IP</td>
<td>VoIP, Wireless</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Device</td>
<td>End-to-End</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>Best of breed by technology</td>
<td>Integrated platform</td>
</tr>
<tr>
<td><strong>Ultimate Goal</strong></td>
<td>Enable visibility</td>
<td>Reduce risk and Ensure business continuity</td>
</tr>
</tbody>
</table>
How can Enterprises assure a Proactive Security Management?

DEAL WITH TWO PARAMOUNT PARAMETERS IN SECURITY

- REDUCE THE POTENTIALITY OF AN ILL WILL → PREVENTION SERVICES
- REDUCING THE IMPACT OF AN ILL WILL → REACTION SERVICES
What Do Our Security Services Solve?

Our security services play a role in each and every step of a Customer project.

- Threat Prevention & Management
- Security Monitoring
- Crisis & Incident Management
- Risk Assessment
- Business Impact Analysis
- Gap Analysis
- Vulnerability Assessment
- Penetration testing
- Secure Architecture Review
- Compliance Readiness
- Security Policy & Program Development
- Security Architecture & Design
- Security Policy & Integration
- Business Continuity Planning

- Remediation
- Deploy Security Systems/Elements
- Business Continuity Plan Testing
- Ongoing Management
- Analysis & Planning
- Consult
- Design
- Integrate
- Deploy
- Maintain & Operate
Security Services Concept

Threat Management Center activity as a Control Tower

- Insure a permanent monitoring of the activity
- Define the access point to the resources and filter the exchanges
- Establish security perimeter
- Protection of the critical resources
- Setup passive protections
- Training of the team
- Prepare the methods of reprisals

from the concept of castle to airport

(INFORMATION HUB)
2
Proactive Security Management: Prevention Portfolio
Security Policy Development

*Defines and documents expected position on security, and use of technology and resources, using industry standards to provide benchmarks*

**What we do:**
- Analyze present security environment
- Document policy findings and security requirements
- Prioritize recommendations for corrective action
- Formulate and document security policies
- Develop a Business Continuity Disaster Recovery plan tailored to your business needs

**What we deliver:**
- Written analysis of security requirements and recommendations for an ongoing security program
- Statement of vulnerabilities, comparing security policies to business requirements
- Documentation of security needs and recommended practices for integration into site security policies
- Prioritized high-level recommendations identifying areas for security improvements

Senior Consultants certified CISSP ISO27001 ...Pragmatic Approach
Analyzes, designs and configures your security architecture, creates policies, and deploys security systems/elements - covers new technology concerns as well as migration, optimization scenarios

What we do:

- **Planning:** Analysis of business drivers and security requirements; Definition and evaluation of high-level design
- **Design:** Design of security architecture using best-in-class security components and security policies; documentation and modeling of the detailed design
- **Implementation:** Completion of all security implementation and testing activities, with minimal impact to operations in migration scenarios
- **Operations:** Fine-tuning of technologies as needed

What we deliver:

- Vendor-agnostic list of recommended security components for purchase
- Detailed security design documentation of installed security components, configurations and architecture
- Completion of security implementation and testing activities
- Knowledge transfer to provider’s staff for continued operations support
- Recommendations for further security component enhancements

Long experience from complex environment, Products Certifications, PM Background;
Security Assessment

A comprehensive assessment of your organization and network that reveals security exposures and defines mitigation options

What we do:
- Review your security policies and understand their current application through interviews and audits
- Identify gaps between the industry standards (e.g., ISO 27001, ISO 17799, etc.) and your current security posture
- Identify deviation from BCDR policies and industry best practices;
- Assess current security technical architecture
- Penetration Tests with Zero or Full Knowledge Penetration

What we deliver:
- Security Compliance Readiness Report
- Documentation of baseline security posture
- Network scanning results
- Prioritized Threat Matrix
- Knowledge transfer for your staff
- BCDR plan and testing scenarios
- Tailored mitigation recommendations

First to do it in France, Global offer to fulfill customer’s objectives, Pragmatic approach, Secret Classified Consultants
Threat Management

Identifies broad threats, as well as environment-specific vulnerabilities and corrective measures, and delivers customized reporting from 24/7 security monitoring, incident handling and crisis management expertise

What we do:

- Analyze broader threat activities, and assess which vulnerabilities are applicable to and will have impact for your environment
- Provide 24/7 monitoring and customized reporting
- Perform trending and analysis of logs and security threat activities
- Provide event notification and recommendations for mitigation strategies, or corrective measures
- Handle escalations for incidents and crisis management as needed

What we deliver:

- Vulnerability assessment and scanning reports
- Attack simulation and service impact analysis
- Real-time advisories
- Security events notification through log file correlation and analysis
- Customized reporting through web portal

Costs optimization (skills sharing) - Secret Classified & technical certified. Synergy between Cert-IST consultant & support teams. All customer information logs are stored in Europe. Large delivery to Technical people up to CIO
Threat Management Center services overview

**Threats & Vulnerabilities Management**
- **PREVENTION**
  - WATCH
  - ASSESS
  - ASSURE
- **DETECTION**
  - DETECT
- **REACTION**
  - ALERT
  - REACT
  - INVESTIGATE

**Event & Incident Management**

**Services**
- Customer portal
- Service Desk (ABUSE)
- DASHBOARDS / REPORTING

**Support**
- Training / sensibilization
- Infrastructure & Infostructure

**Accompaniments services with results engagements (SLAs)**

**Services**
- Trouble interface
- Incident interface
- Change interface
- Config. interface
- Service Level Mgt
Threat Management PROGRESSIVE APPROACH

1. FOLLOW-UP OF THE TOPICALITY (DAY BEFORE)
   - What does it occur in my environment?

2. INVENTORY OF FIXTURES (RESEARCH VULNERABILITIES)
   - Where am I vulnerable?

3. ANALYZE IMPACTS (IDENTIFICATION OF THE RISKS)
   - Which are the impacts in my environment?

4. DEFINITION OF COUNTER MEASUREMENTS (COHERENCE BEFORE DEPLOYMENT)
   - How to save time and to assign my resources to the good place and the good moment?

5. FOLLOW-UP PATCH MANAGEMENT (IMPACT DEPLOYMENT)
   - How does the application do without the corrective measures?

6. ANALYZE RESIDUAL RISK (FOLLOWED ACTION PLAN)
   - On what is necessary it to maintain the monitoring?

7. FOLLOW-UP OF THE TOPICALITY (DAY BEFORE)
   - What does it occur in my environment?
Threat Management Deliveries

WATCH
- Take care on the threats and the vulnerabilities
- Monitoring of the vulnerabilities according to the reference frame customer
- Analyzes impact
- Recommendations with the identified vulnerabilities
- Reporting

ASSESS
- Recovery of the existing configurations at the customer
- Identification of the vulnerabilities
- Simulation of attacks
- Analyze impact
- Recommendations with identified vulnerabilities which can be exploited
- Reporting

ASSURE
- Recovery of the existing configurations at the customer
- Identification of the vulnerabilities
- Follow-up of the requests (workflow)
- Analyze impact
- Recommendations with the requests for change
- Reporting
Threat Management: Cert-IST

- **Ability to distribute security alerts in a timely fashion to Customers** (e.g. critical new vulnerability in Oracle, new worm propagating, ...)
- **Support on ICT incident handling** *(crisis management with Alcatel-Lucent crisis hub)*
- **Major role in the Security monitoring & Threat management service**
- **Key differentiator towards competition**

### Diagram

- **Threats and flaws**
- **Operator**
- **Incident**
- **Business / Mission Continuity**

- **Early Detection**
  - «Watcher»

- **Alerts & Advisories Release**

- **Incident Response**

- **Database & Tools**
  - Vulnerabilities
  - Risk Classification
  - Advisories/Alerts
  - Investigation/Mgt
The Process: Vulnerability monitoring

Information collection and qualification

Collection
- e-mail lists
  - Editors
  - Vendors, Full Disclosure
  - FIRST
  - Certs FR and other
  - Underground, EISPP

Web observer
- Editors
- Vendors
- Others security sites
- Press

Qualification

Alert
- DANGER
- Advisory
- Virus-Coord
- Under analyze
- Monthly bulletin

1. Other information collection (products, vulnerabilities,...)
2. Risk assessment
3. Vulnerability testing / Exploit testing / Patch analyzing
4. Log book
5. Classification of the information

Vuln_Coord

risk

1- Other information collection
2- Risk assessment
3- Vulnerability testing / Exploit testing / Patch analyzing
4- Log book
5- Classification of the information
Service Risk Management (8649 SRM): Conceptual Overview

8649 SRM is a software package that:

- Delivers high level, security specific alarms
- Defines clusters for priority actions according to nature of risks
- Provides solutions to isolate and remediate vulnerabilities according to business processes priorities
- Provides a mechanism to verify regulatory policy compliance

8649 SRM includes a service component that:

- Regularly updates the 8649 SRM vulnerability database
- Keeps the system current and up to date

8649 SRM:

- Integrates with the Operator and Enterprise Network and Systems Management Platforms
- Incorporates a data description of Business Processes
Service Risk Management System

**Primary Uses:**
- Vulnerability Modeling & Mitigation

**Key Benefits:**
- Improved Decision Making
- Decrease Cost of Vulnerability Mgt
- Improved security responsiveness
- Improved business alignment

**How It Works:**
- Builds a physical model - existing data
- Overlays business service relationships
- Analyzes against known vulnerabilities
- Aggregates vulnerabilities - prioritizes

**Other Features:**
- Integrates with existing ticket systems
- Simulations - what if scenarios
- Detailed ad-hoc and pre-set reports
VitalSuite® Performance Management

1. **Fully integrated** management of network, services, applications and business performance
2. **Flexible and scalable** solution that grows with your network
3. Out-of-the-box solutions with **extensible support**
4. **Web GUI** provides access to real-time, infrastructure wide network transport and business application performance data
5. **Rapid deployment** for quick return on investment and delivery of services
Example 1: Ensure VoIP quality from day 1 till full deployment

**Goal:** Ensure QoS for a new VoIP deployment from day 1 and pro-actively upgrade the network if needed

**Problems:** How do you predict problems before they occur? How do you know what part of the network needs to be upgraded?

**Solution:**

Pre-day Day 1:
- VoIP readiness assessment through synthetic agents
- Start monitoring network performance (capacity, delay,...)

From day 1:
- Monitor VoIP QoS from live calls as well as synthetic agents
- Zoom in on weak point in the network and plan changes to the network BEFORE they become a bottleneck affecting the VoIP QoS
Example 2: Ensure excellent response times for crucial applications

**Goal:** Ensure employees and customers can work efficiently

**Problem:** How do you predict problems before they occur? How do you know if the weak link is the PC, the network or the server?

**Solution:**
- Monitor Application response time from the end-user perspective
- Generate alerts when response time slows down
- Get reports that show if the weak spot is PC, network or server
Example 3: Minimize business interruptions during and after a security attack

**Goal:** Ensure normal business can go on while dealing with a security attack

**Problem:** Do you know if your crucial business applications remain available during an attack? How can you be sure that a new security patch or firewall settings doesn’t prevent end-users from accessing business critical applications?

**Solution:**

- Monitor Application response time from unmanned PC’s and apply new patches or settings first on these PC’s before deploying them on life system
- Generate alerts when the server is not reachable or response time slows down
- This can be combined with monitoring application response time from the real end-user PC’s
MyVital Portal:
Customer Network Management
Self Care with individualized, secure views
Immediate sectionalization of problems

VitalNet™
Trend Analysis
SLA Reports

VitalNET Realtime
Path Analysis

VitalApp™
View of End User Experience
Patented Agent Technology

VitalSuite® Performance Management
Network, Service and Application Monitoring from a customer perspective
VitalSuite® Network Performance Management (VitalNET)

Monitor, analyze and predict network infrastructure behavior

Benefits

1. Network-wide visibility
2. Fast, easy deployment with out-of-the-box reports
3. Preempt problems - enhance end user satisfaction
4. Protect investments
   - Integrate existing & emerging technologies, VoIP, SANs, etc.
   - Scalable for cost effective price/performance
   - Immediate ROI - lower operations & ownership costs

Reduce Operation & Capital Expenses

VitalSuite® Comprehensive Data Collection

- Servers
- Routers
- EMS/Probes
- Toolkits
- SNMP MIBs

Anywhere WEB Access
Pin-point problems at-a-glance
Capacity Planning Trend Analysis
Personalized Views
SLA Reports
VitalNET - Real Time Module

Enable real-time performance and service management

Benefits

1. Network-wide visualization
   - Wide adaptability of views, thresholds, notification

2. Reduced operations costs
   - Multi-vendor, multi-technology investment protection
   - Rapid problem identification and resolution

3. Immediate event notification
   - Detects problems in real-time before they affect users

4. Enhanced customer satisfaction
   - Prevent service impacting problems

Event Analysis
- SNMP Mibs
- SLA Violations
- Traps
- ATM, FR, IP/MPLS, VoP
- Proactive Identification
VitalSuite® Application Performance Management (VitalApps)

Monitor, Analyze and Predict Network QoS and Application Behavior

Benefits

1. Unprecedented visibility from the end-user’s perspective
   - Service level management for Wireless WANs/WLANs, Enterprise Applications and LAN
   - Exposes IPSec VPN setup and operational performance

2. Passive and active network testing and assurance

3. Scriptable, distributed Agents verify performance on key paths through the infrastructure

4. Built-in VoIP network tests
VitalApps example:
Monitoring Performance from Multiple Vantage Points
VitalSuite® Advanced Reporting Toolkit (ART)

Customize reporting, simplifies service management

Benefits

1. Service level verification
2. Capacity planning for intelligent budgeting
3. In-depth, proactive problem resolution
4. Fast, flexible report creation
   - Integrated, comprehensive data reporting
   - Up-to-date, extensible data
   - Complete report administration package
5. Out-of-box reports

VitalApps™ Application and Alarm Analysis

-VitalSuite® Advanced Reporting Toolkit (ART)
Executive Summary: VitalSuite

- ROI over 500% (customer case studies)
- Payback period 3-5 months (IDC study)
- Solutions proven at over 400 customers in EMEA over 1000 worldwide
- Market Leading Solutions deployed at 75% of Fortune 100 companies
- Award Winning Solution!
3

Proactive Security Management: Reaction Portfolio
Threat Management Center services overview

- **DASHBOARDS / REPORTING**
  - Customer portal

- **Service Desk (ABUSE)**

- **Threats & Vulnerabilities Management**
  - PREVENTION
  - DETECTION
  - REACTION

- **Event & Incident Management**
  - WATCH
  - ASSESS
  - ASSURE
  - DETECT
  - ALERT
  - REACT
  - INVESTIGATE

- **Training / sensibilization**

- **Services**
  - CRISIS MANAGEMENT
  - Trouble interface
  - Incident interface
  - Change interface
  - Config. interface
  - Service Level Mgt

- **Infrastructure & Infostructure**

- **Accompaniments services with results engagements (SLAs)**

All Rights Reserved © Alcatel-Lucent 2007
Reaction

From the bottom to the top:

1. **Event Management**
2. **Alert Management**
3. **Incident Management**
4. **Metrics**
5. **Comparative Metrics**
6. **Incident Resolution**
7. **Alerts Monitoring**
8. **Control Monitoring**
9. **Reports**
10. **Executive Management**
11. **CIRT**
12. **Security Operations**
13. **Internal & External Auditors**

**Other Measures**

**Other Manager Alerts**

**IT Best Practices**

**Devices**

**DATA**
Origin of the Logs

Collected, treated and analyzed in France Alcatel-Lucent

+70 countries out of the 5 continents
Threat Management Center: PROGRESSIVE APPROACH

- Analyze Trade (Multi Devices & Other Indicators)
- Analyze Service (Multi Devices)
- Analyze with Vulnerabilities Insertion
- Analyze Device
- Statistics
REACTION / REPRESENTATION Operational View

This graph displays the number of alerts, classified by severity (five levels: high, medium, low, info, unknown), for each site, split by severity.

This graph shows the average number of alerts per hour for each day of one week.

This graph displays the number of alerts for each month of one year, split by severity.

This graph displays the number of alerts for each sensor type.
Alcatel-Lucent Responses

<table>
<thead>
<tr>
<th>Security domain</th>
<th>Monitoring control class</th>
<th>Most representative problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREVENTION</td>
<td>SERVICE QUALITY</td>
<td>Equipment malfunction</td>
</tr>
<tr>
<td></td>
<td>VULNERABILITY</td>
<td>Equipment self-protection weakness</td>
</tr>
<tr>
<td></td>
<td>CONFORMITY</td>
<td>Equipment bad configuration</td>
</tr>
<tr>
<td>REACTION</td>
<td>MALICIOUS INTENT</td>
<td>Attacks</td>
</tr>
<tr>
<td></td>
<td>USAGES</td>
<td>Bad or abnormal user behavior</td>
</tr>
</tbody>
</table>
REACTION / REPRESENTATION Decisional view
Strategic view
Establishes an incident management system, providing your staff with techniques, procedures and operational plans for handling incidents

What we do:

- **Planning**: Analysis of current security architecture, policy and plan development, and identification of internal resources
- **Design**: Identification of technical infrastructure, design of processes and utilization of existing technologies for development of communication, reporting and management processes
- **Implementation**: Incident preparedness and processing, internal training and information deployment, CERT services customization
- **Operations**: Incident response program maintenance, possible staff augmentation and creation of onsite emergency team, crisis management

What we deliver:

- Policy and process documents defining procedures and communication standards
- Plan for distributing and maintaining the incident response program
- Incident response policy and functional architecture based on industry best practices and CERT expertise

Expertise - Neutrality - Strong process - Active Collaboration with SRPJ, OCLCTIC ...
You’re all welcome to visit the Alcatel-Lucent worldwide TMC Center!
4

Questions / Answers
Build a rich and successful relationship with Alcatel-Lucent