Managed Security Services

What is on the truck

Managed Security Services

Professional Services

Security Hardware and Software
Agenda

An introduction and statement of capability

Virtual SOC – Service delivery

Managed Security Services
- Managed Firewall, IDS, IPS, UTM Services
- Managed Protection Services
- Service Level Agreements
- Identity and Access Management (IAM) Services
- Managed Data Security Services

Enablement Services
- Security and Event Log Management
- Vulnerability Management Services
- X-Force Threat Analysis Services
- Email and Web Security

Power of the Integration

Customer Portal

Conclusion
An introduction and statement of capability
16 Years of Innovation

**1992** – First Vulnerability Detection System (Shareware)

**1994** – First commercial vulnerability scanner (Internet Scanner)

**1996** – First Intrusion Detection System (RealSecure)

**1998** – First integrated host/network security solution

**1999** – First correlation SMS (Safesuite Decisions)

**2001** – First IPS & Site Protector Management

**2004** – Enterprise Security Platform

**2005** – ISS MSS
  “Magic Quadrant Leader”

**2006** – Proventia
  Enterprise Scanner & ADS

**2007** – ISS MSS
  “Magic Quadrant Leader”

**2006** – ISS MSS
  “Magic Quadrant Leader”
Only IBM Security is backed by the IBM X-Force research team

Research

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

Technology

- X-Force Protection Engines
  - Extensions to existing engines
  - New protection engine creation
- X-Force XPU’s
  - Security Content Update Development
  - Security Content Update QA
- X-Force Intelligence
  - X-Force Database
  - Feed Monitoring and Collection
  - Intelligence Sharing

Solutions

- Managed Security Services
- Professional Services
- Security Hardware and Software

The X-Force team delivers reduced operational complexity – helping to build integrated technologies that feature “baked-in” simplification
Virtual Security Operations Center (VSOC)

Managed Security Services
- Managed and Monitored Firewall Services
- Managed Identity Services
- Managed IPS and IDS Services
- Managed UTM Services
- Managed Protection Services for Networks, Servers and Desktops

Security Enablement Services
- Vulnerability Management Services
- Security Event Management Services
- Secure Log Management Services
- IBM ISS X-Force® Threat Analysis Services
- Managed E-mail Security
- Managed Web Security

Multiple Device Types & Vendors Supported
Global Security Reach and Expertise

- 8 Security Operations Centers
- 7 Security Research Centers
- 133 Monitored Countries
- 20,000+ Devices under Contract
- 3,700+ MSS Clients Worldwide
- 4 Billion+ Events Per Day

Additionally:
- 3,500 - 4,000 Practitioners Worldwide
- Thousands of PSS engagements delivered annually
- Global and local PSS security expertise
Internet Security Systems – Virtual SOC

Best-of-Breed Security Platform Support
Sytrust & SAS-70 Certified SOC
Security Incident Escalation
Completely Web-Driven Interface
Standard & Customizable Reporting
Industry Leading Performance-based SLAs
Access to Security Intelligence (XFTAS)
24/7 Expert Monitoring and Management
Managed Security Services
Deployment & Services for Email & Web

In the cloud
Email Anti-Virus Anti-Spam
Image & Content Control

In the cloud
Web Anti-Virus Anti-Spyware
URL Filtering
World Class: People, Processes and Technology
Managed Security Delivery Organization

**Deployment & Integration**
- Global Service Deployment
- Project Management

**Security Operations Center**
- 24x7 Global Delivery Operations
- Focused Workload

**Customer Advocacy**
- Customer Relationship Management
- Global Presence

**Engineering**
- SOC Tools & Portal Development
- Dedicated Infrastructure Management

**Threat Intelligence**
- Dedicated MSS Intelligence
Managed Security Services (MSS)
**Key Benefits**

- Protect company assets, brand reputation and business continuity with 24x7 reliable monitoring and management
- Reduces in-house security costs by up to 55 percent
- Achieves security compliance with industry and governmental regulations
- Maximizes existing security investments
- Improves productivity by freeing IT resources to focus on strategic initiatives
- Reassures clients, partners and shareholders that critical data is protected by trusted resources
- Reduces operational complexity
Managed Services: Managed Security Services (MSS)

Industry Proven Managed Security Services
- Managed Intrusion Detection/Prevention Service
  - Network, Server/Host
- Managed Firewall
- Unified Threat Management (UTM)
  - Customizable support for best-of-breed multi-function devices
  - Protection (FW-VPN/IPS) and/or Content (URL Filtering/AV/AntiSpam) packages

Multi-Vendor Security Technology Support
- IBM ISS, Cisco, Juniper
- McAfee, Sourcefire
- CheckPoint

Best-in-Class Service Level Agreements

Multiple Service Level Options
- Standard, Select, Premium

Industry Leading Customer Portal
Embedded X-Force Intelligence
Managed Security Services (MSS)

*If you remember one thing…*

Best of Breed Technology Support
10 Years of Experience
Industry Leading SLAs
MSS Portal included
XForce Integrated
Managed Services: Managed Protection Services (MPS)

**Guaranteed Protection**
Based on IBM ISS Security Technologies
- Proventia G (ID/PS)
- Proventia Server
- Proventia Desktop

Best-in-Class Service Level Agreements
- Performance based SLAs

Multiple Service Level Options
- Standard, Select, Premium
- Choose services per device for custom solutions

Industry Leading Customer Portal
Embedded X-Force Intelligence
Managed Protection Services (MPS)

If you remember one thing...

Protection SLA Guarantee

*up to 25,000 €*

Warranty Program

*up to 50,000 €*

Performance Based SLAs
Service Level Agreement (SLA)
Managed Security Services

Provides **Breadth of Coverage**

Across a Diverse set of Markets

<table>
<thead>
<tr>
<th>Device &amp; Policy Management</th>
<th>AI Alerting</th>
<th>Eyes On Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSS Standard</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MSS Select / Premium Or with Event monitoring option</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Managed Security Services SLAs

Security Incident Prevention
- All exploits on the X-Force Certified Attack List (XFCAL) will be blocked.

Security Incident Identification
- All priority 1, 2 and 3 level security incidents will be identified by the SOC.

Security Incident Response
- All security incidents will be escalated within 15 minutes of identification.

Intrusion Event Countermeasure
- Countermeasures will be implemented 30 minutes after customer approval for all priority 1 incidents.

Policy Change Acknowledgement
- All policy changes will be acknowledged within 2 hours of receipt.

Policy Change Implementation
- All policy changes will be implemented within 8 hours of receipt (Select Level).

Proactive System Monitoring
- 15 minute customer notification of any MPS device unreachable.

Proactive Security Content Update
- Security content updates will be applied within 48-hours of release.

Customer Portal
- 99.9% accessibility to the MSS customer portal

Internet Emergency
- 15 minute notification of the declaration of an Internet Emergency.

The industry’s first and only SLAs with “skin in the game”
Identity and Access Management Services
Data Security Services
IBM ISS Identity and Access Management (IAM) Services

Providing security-rich access to business assets and resources

- **Identity assessment and strategy services** give organizations an understanding of the current state of their identity management environment and provides a strategy and roadmap for improving their current IAM posture.

- **User Provisioning Services** help clients set up, secure and manage the lifecycle of their user accounts leveraging IBM Tivoli® Identity Manager Software.

- **Web Access Management Services** help organizations manage and validate user access to devices, applications and systems leveraging IBM Tivoli Access Manager software.

- **Enterprise Single Sign On Services** help organizations relieve password headaches with Tivoli Access Manager for Enterprise Single Sign on -- a proven single-sign on solution across all network access points.

- **Managed Identity Services** provides a secure identity management solution, through either an IBM hosted or client premise model, that supports compliance while enabling collaboration across a diverse user base.
IBM ISS Data Security Services

Reducing cost and complexity of data protection by managing and optimizing across key control points

1) Enterprise Content Protection (ECP)
   - Network Data Loss Prevention (DLP)
   - Enterprise Data Loss Prevention (DLP) (Endpoint DLP + Network DLP)

2) Endpoint Data Protection (EDP)
   - Endpoint Encryption
   - Endpoint Data Loss Prevention (DLP)

3) Activity Compliance Monitoring & Reporting (ACMR)
   - Log Analysis Management

Requirements and planning workshop
Discovery Assessment
Policy Design
Implementation
Enablement Services
Key Benefits

- Centralized command center to monitor and control Virtual-SOC services
- Run queries and generate reports on multi-vendor security devices, security events, service level agreement (SLA) activity and more
- Automated analysis of security events and logs alerts for remediation
- Unlimited archive system stores one year of online event/log storage and seven years of offline archiving
- Authorized access to portal for increased internal protection
- Integrated with X-Force security intelligence feeds and daily threat assessments
Enablement Services: Security Event & Log Management

Log and Event Collection & Archival
- Syslog, Universal Logging Agent (ULA)
- On Site Aggregation, Compression, Encryption
- Secured Communications
- Forensically Sound Storage

Automated Alerting (Select Level Only)

SOC Event monitoring -
Security Incident Tracking
Industry Leading Customer Portal
Embedded X-Force Intelligence
Log storage upto 7 years
Compliance Reporting
- Windows & Linux
### MSS SELM “Comparison”

<table>
<thead>
<tr>
<th></th>
<th>Device + Policy Management</th>
<th>AI Alerting</th>
<th>Eyes On Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MSS Standard</strong></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>MSS Select / Premium Or with Event monitoring option</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SELM Select + SOC Event Monitoring</strong></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Enablement Services: **Vulnerability Management Systems**

Internal & External Vulnerability Assessments
Vulnerability Remediation Workflow Embedded
- Step-by-step Remediation Actions
- Complete Ticketing System
- Virtual Patch ties to MPS/MSS

Granular Access Control & Permissions
Fully functioned Reporting
Industry Leading Customer Portal
Embedded X-Force Intelligence
Enablement Services: X-Force Threat Analysis Service

X-Force Threat Analysis Service

- News
- Vulnerabilities
- Exploits
- Worms/Virus

Breaking Security Intelligence Alerts
Configurable Alerting/Advisories
Daily Emails
Direct Feed from X-Force Research

- 30,000+ Records
Managed Email & Web Security Services
Managed E-mail Security

- 100% Virus Protection
- 99.2% Spam Effectiveness with 1 in 1 Million False Positives
- 90%+ effective in identifying pornographic attachments
- Enforces Acceptable Use Policy
- Multiple Layers of Defense
- Highly redundant infrastructure
- Assists in stopping confidential information leaving your company
- Industry Leading Performance-based SLAs
Managed Web Security

Features: Web

- Converged Threat Analysis, taking recent threat information from other protocols such as email and applying that knowledge to web transactions
- Global load balancing optimizes web traffic filtering and provides network level fail-over
- Multiple layers of defense
- Industry-leading SLAs on service availability
- Visibility of activity at the user level without the need for software installed on every client
- Comprehensive on demand reporting (summary and detailed reports), auditing and dashboard
- Easy to configure and deploy
The power of the Integration
Integrated Services

What You Get:

- Single view to overall security posture
- Integrated data sets across the entire breadth of services
- Correlation regardless of device type or vendor
- Integrated vulnerability management capabilities for improved accuracy and better protection
- Virtual Patching capabilities for streamlined remediation
- Automated event escalation
- Built-in security intelligence
Scan network to detect vulnerabilities.

Use the Virtual-SOC portal to request application of patch updates to protect entire network or individual servers.

Upon receipt of the patch request, an IBM ISS SOC analyst will implement an IPS rule, if applicable; to block access to the specific vulnerability and apply protection for the system until it is patched.

Managed Protection Services with Vulnerability Management Services
Managed Intrusion Detection/Prevention Service with the Managed Firewall Services

1. If IBM ISS monitors and manages firewall and intrusion detection/prevention, and an attack is verified...

2. IBM ISS requests authorization to implement changes to firewall rules and/or IPS policies to prevent access from malicious hosts.
The Power of Integrated Services
“MSS in Action”

Security Event & Log Management Services & Managed Intrusion Detection/Prevention Services or Managed Firewall Services

1. IBM ISS provides the ability to manage, monitor, or view all of the customer’s firewall, IDS and IPS devices.

2. IBM ISS provides customers with a consolidated security view and full reporting capabilities.

3. Customers can access secure log/event archival of all aggregated security events for up to 7 years.

4. Customer can leverage combined trouble ticketing capabilities to track issue resolution transparently across managed and unmanaged devices.
The Power of Integrated Services
“MSS in Action”

X-Force® Threat Analysis Service and Vulnerability Management Services

1. Schedule automated scans to identify OS’s, applications, and their respective vulnerabilities.

2. Scan results dynamically reconfigure the customer’s XFTAS alerting preferences, providing real-time alert notifications for actionable vulnerabilities.

3. Remediation workflow management features of the VMS service allow for generation of tickets for vulnerable assets with powerful grouping and prioritization capabilities.

4. Validated remediation tasks have been completed by re-scanning of vulnerable assets.
X-Force Means Better Protection For ALL MSS Clients!

*Proof point: Widespread SQL Injection Attacks of 2008*

- MSS and X-Force collaborated to monitor outbreaks of SQL injection and detect variants during the second half of 2008.
- **MSS clients using IBM ISS Proventia devices were preemptively protected** from SQL Injection attacks via X-Force security updates.
- **MSS clients using security devices from other vendors were protected** thanks to collaboration with X-Force to create non-public custom detection signatures specifically for MSS clients.
Customer Portal
MSS Customer Portal: Dashboard

- Full Portal Searching
- Daily Threat Assessment
- Recent Security Incidents & Service Requests
- 7 Day / Daily Trends
- Security News, Bulletins and Intelligence Quick Links
Portal Real-Time Events: Device Management Policies View

Live event monitoring can be done via the Active Analyzer function on the Logs menu. The Active Analyzer can be set to Auto-refresh every 30 seconds or manually via single click.

IDS
Firewall
Anti-Virus
Anti-Spam
Web-Filtering Policies
MSS Customer Portal: Real-Time Log view

- IDS, Firewall, VPN, AntiVirus, AntiSpam, URL Filtering Logs Available
- Drill down feature
- Normalized Logs or Raw Logs.
Log & Event Archival Queries

Log Query

Query Criteria
- Select saved criteria
  - Delete

1. Date/Time
- Start Date: 07/03/2009 11:02:33
- End Date: 07/03/2009 15:02:33
- Start Time: 07/03/2009 11:02:33
- End Time: 07/03/2009 15:02:33
- Time Interval: [ ] Range of time
- Timezone: [ ] GMT-05:00 Brussels

2. Devices Included in Query
- Select a device group
  - No devices, select a device group.

3. Applications
- [ ] Firewall
- [ ] Logins
- [ ] SMS
- [ ] Anti-Virus
- [ ] Anti-Spam
- [ ] URL Filtering
- [ ] Universal Log
- [ ] System Activity

4. Options
- [ ] Include inactive devices (*)
- [ ] Logs per page: 100
- [ ] Resolve DNS: [ ] No
- [ ] Sort Type: Oldest first
- [ ] Save this criteria

5. Full Text Search
- Search Terms

6. Filters
- [ ] Action: [ ]
- [ ] Source IP: [ ]
- [ ] Destination IP: [ ]
- [ ] Protocol: [ ]
- [ ] D. Port: [ ]
- [ ] C.
- [ ] Firewall Rule: [ ]
- [ ] IDS/IPS Priority: [ ] Low, [ ] Medium, [ ] High
- [ ] Anti-Virus Attack: [ ]

7. Include inactive devices (*)

8. Universal Log
- Log File:

9. URL Filtering
- URL:

10. System Activity
- User Name:
- Regular Expression:
X-Force Protection System (XPS)

Normalization; Aggregation; Correlations; Categorization; Prioritization

Correlations
- Cross platform
- Historical & Statistical
- Asset : Internal
- Asset : Authorized Scanner
- Asset : criticality
- Vulnerability & OS
- XPS Alerts IDPS
- XPS Alerts Firewall

IBM ISS Manages Third-Party Technologies

Example: typical customer environment

1 Billion

150,000

300

6
Live event monitoring can be done via the Active Analyzer function on the Logs menu. The Active Analyzer can be set to Auto-refresh every 30 seconds or manually via single click.

Changes in event baselines are reflected in the Active Analyzer by highlighting the event row and displaying deltas for event counts, sources and destinations between refresh periods.
MSS Customer Portal : Real-Time Meta events

### Ticket Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Number</td>
<td>885368</td>
</tr>
<tr>
<td>Created On</td>
<td>08/01/2007 23:38</td>
</tr>
<tr>
<td>Last Modified On</td>
<td>12/05/2007 16:01</td>
</tr>
<tr>
<td>Status</td>
<td>New</td>
</tr>
<tr>
<td>Priority</td>
<td>Low</td>
</tr>
<tr>
<td>Resolution</td>
<td>N/A</td>
</tr>
<tr>
<td>Notification Status</td>
<td>No Remote Notification</td>
</tr>
</tbody>
</table>

### Issue Details

**Reason for Exclusion:** Suspicous Activity

**Device Name:**

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
</table>

**Source IP Block Owner:** Multiple

**Destination IP Block Owner:** Multiple

---

200% increase

---

200% increase

---

MSS Customer Portal : Real-Time Meta events

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Number</td>
<td>885368</td>
</tr>
<tr>
<td>Created On</td>
<td>08/01/2007 23:38</td>
</tr>
<tr>
<td>Last Modified On</td>
<td>12/05/2007 16:01</td>
</tr>
<tr>
<td>Status</td>
<td>New</td>
</tr>
<tr>
<td>Priority</td>
<td>Low</td>
</tr>
<tr>
<td>Resolution</td>
<td>N/A</td>
</tr>
<tr>
<td>Notification Status</td>
<td>No Remote Notification</td>
</tr>
</tbody>
</table>

### Issue Details

**Reason for Exclusion:** Suspicous Activity

**Device Name:**

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
</table>

**Source IP Block Owner:** Multiple

**Destination IP Block Owner:** Multiple
MSS Customer Portal: XPS Alerting

- **Correlation Rules**
- **Data Mining Rules**
- **System Activity Rules**
MSS Customer Portal : XPS Alerting

XPS Alert Details

Alert ID: 606048
Start Time: 01/4/2008 01:12:00 GMT
Last Update: 01/4/2008 04:10:16 GMT
Device List: ceri-a280 (Proventia - G 3rd floor)

Rule Name: BackdoorDetectionRule (Intelligent)
End Time: 01/4/2008 01:53:00 GMT
Status: Normalized
Ticket ID: None

Description

Source 208.134.186.22 targeted 12.173.210.59 with an event in the backdoor signature group at Mon Jan 14 01:12:00 GMT 2008 . Triggering event in the category group:
Mstream_Zombie_Request
Source 208.134.186.22 targeted 12.173.210.44 with an event in the backdoor signature group at Mon Jan 14 01:52:04 GMT 2008 . Triggering event in the category group:
Trin00_Daemon_Request
Trin00_Daemon_Request
Source 208.134.186.22 targeted 12.173.210.52 with an event in the backdoor signature group at Mon Jan 14 01:53:00 GMT 2008 . Triggering event in the category group:
Trin00_Daemon_Request

Signature Group Names

scan, backdoor, xferal

Event Names

SocketsDetrie_Request, Mstream_Zombie_Request, WinTrin00_Daemon_Request, Trin00_Daemon_Request, Syphilis_Scan_Request

Sources

Critical: 0 (0%)  Internal: 0 (0%)  Auth Scanner: 0 (0%)
RPC/USER: 0 (0%)  Vulns Present: 0 (0%)
IPs 208.134.186.22

Destinations

Critical: 1 (3%)  Internal: 33 (100%)  Auth Scanner: 0 (0%)
RPC/USER: 0 (0%)  Vulns Present: 31 (93%)
All tickets generated by both ISS and the customer are viewable via the Ticket Manager.

A user-friendly query interface allows for rapid access to specific ticketing data.

All tickets are available on-line for up to one year as a standard component of all ISS Managed Services.
Customer Portal Reporting

The portal reporting engine provides a custom query capabilities that allow users to build reports for exactly the data they desire.

All reports can be run in several formats and can be exported to HTML, CSV and PDF.
Conclusion
Managed Security Services

Guaranteed Protection
- Industry’s leading performance-based service level agreement (SLA) with a cash-back payment enhances overall security posture
- Provides protection from known and unknown threats

Lowers Total Cost of Ownership
- Reduced complexity
  - Integrated services reduces security exposures
  - Virtual-Security Operation Center
- Infrastructure optimization
  - Maximized network uptime, availability, and bandwidth
  - Integration of disparate security technologies
  - Simplification of on-going security management,
  - Improves speed to protection
  - Global, local capability and scalability for optimization of existing infrastructure
- Optimized employee productivity
  - More efficient use of resources
  - 24/7/365 or coverage on nights, weekends, off-hours
  - Built-in security expertise (systems, people)

Helps Demonstrate Compliance
- Satisfies customer internal and regulatory controls
- Process to meet and maintain compliance
MSS - Delivering Value Through Differentiation

Breadth of services
- Monitored and Managed Services, vendor agnostic
- Cloud-based
- Security as a service

Integrated services
- Correlation of security vulnerabilities with events to provide optimized security
- Single management view and control of enterprise-wide security posture
- Integrated executive and technical reporting

Flexible service options
- Maintain as much control as you want—monitored, managed, unmanaged, combination of both
- Protection at your fingertips—nights, weekends, off-hours
MSS - Delivering Value Through Differentiation

Strong Service Level Agreements (SLAs)
- Built on security best practices
- Performance-based – Guaranteed Protection services

Virtual Security Operations Center
- Integrated services architecture combining:
  - Management Portal
  - Integrated X-Force Security Intelligence
  - XPS (Normalization, aggregation, correlation, archival, escalation, remediation)
- Finds the needle in the haystack
- Work flow, ticketing, emergency response and forensics, comprehensive reporting

Security Expertise
- Security is all we do, focused on protection X-Force
IBM Security Recognition
Trusted global security solutions – backed by real industry validation

  - Gartner Magic Quadrant
  - Forrester Wave
  - Frost & Sullivan
- #1 Identity Management Provider, IDC (2007)
- #1 Vulnerability Assessment Provider, Frost & Sullivan (2007)

- Gartner Leaders Quadrant, Network IPS (February 2008)
- Gartner Leadership Quadrant, Web Access Management (October 2007)
- Gartner Leadership Quadrant, User Provisioning (August 2007)
Questions?

Presenter: Collart Marius

marius_collart@be.ibm.com
Title: Service Solutions Expert - Managed Security Services


Thank you!