

IBM **BusinessConnect**

**A new era of thinking.**

#BizCoMaroc

# IBM Security

Votre entreprise est-elle  
suffisamment sécurisée?

Michel Bobillier  
Program Director, Worldwide Security Tiger Team  
May 2016



## AGENDA

1. Common Myths
2. Five Fundamentals
3. Maturity Model
4. Is my SOC optimized

## To address security, leaders must avoid common myths



Your company is not infected. (It is.)



Whatever you've done is enough. (It is not.)



There's a silver bullet to protect you. (There isn't.)



You need to put your company in lock-down. (You don't.)

- Adding another tool
- Hoping it's not me
- Building more barricades
- Skipping the basics
- Ignoring privileges
- Blocking the cloud
- Betting on BYOS

DOES NOT  
WORK !

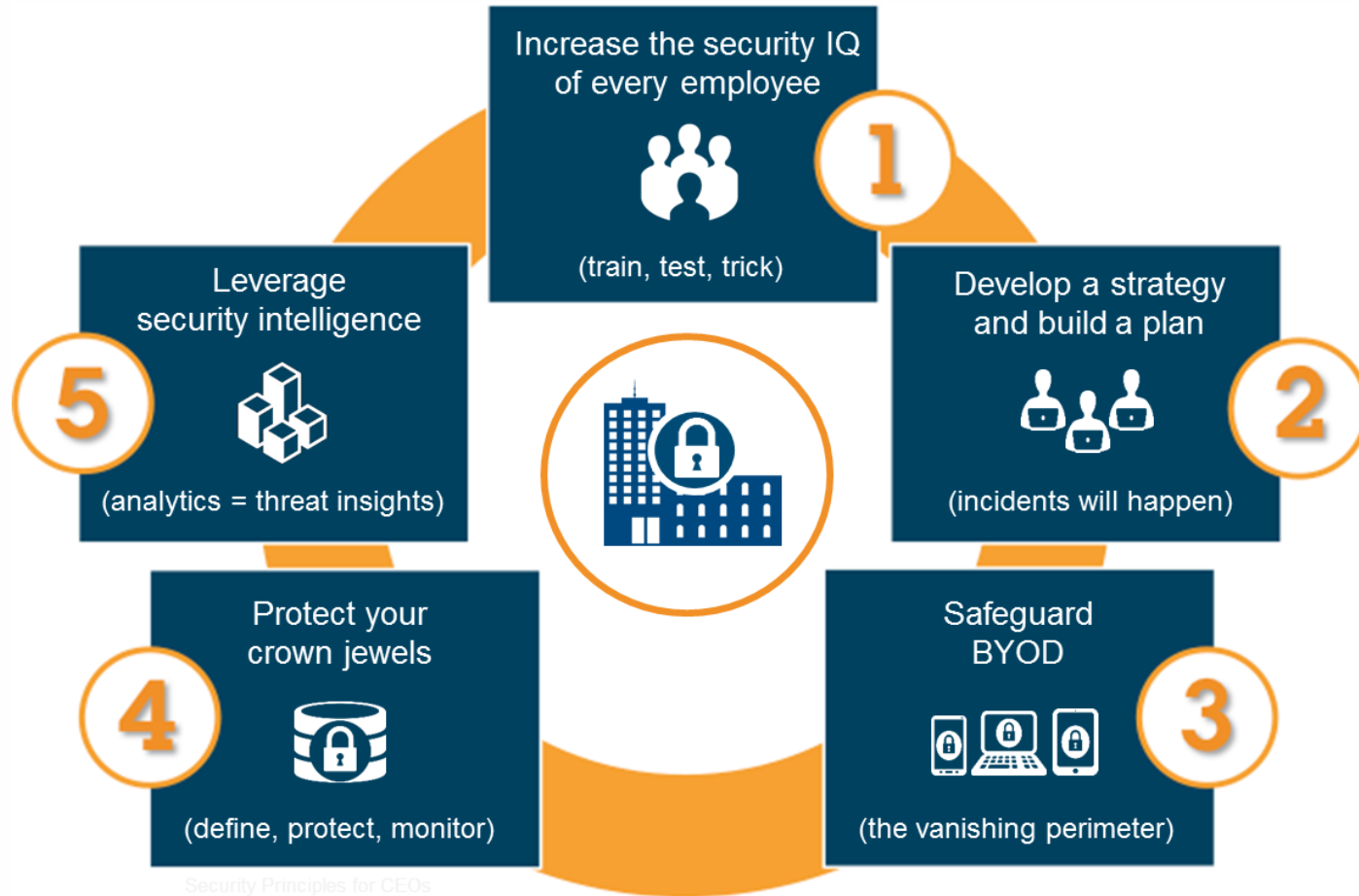




## AGENDA

1. Common Myths
2. **Five Fundamentals**
3. Maturity Model
4. Is My SOC Optimized

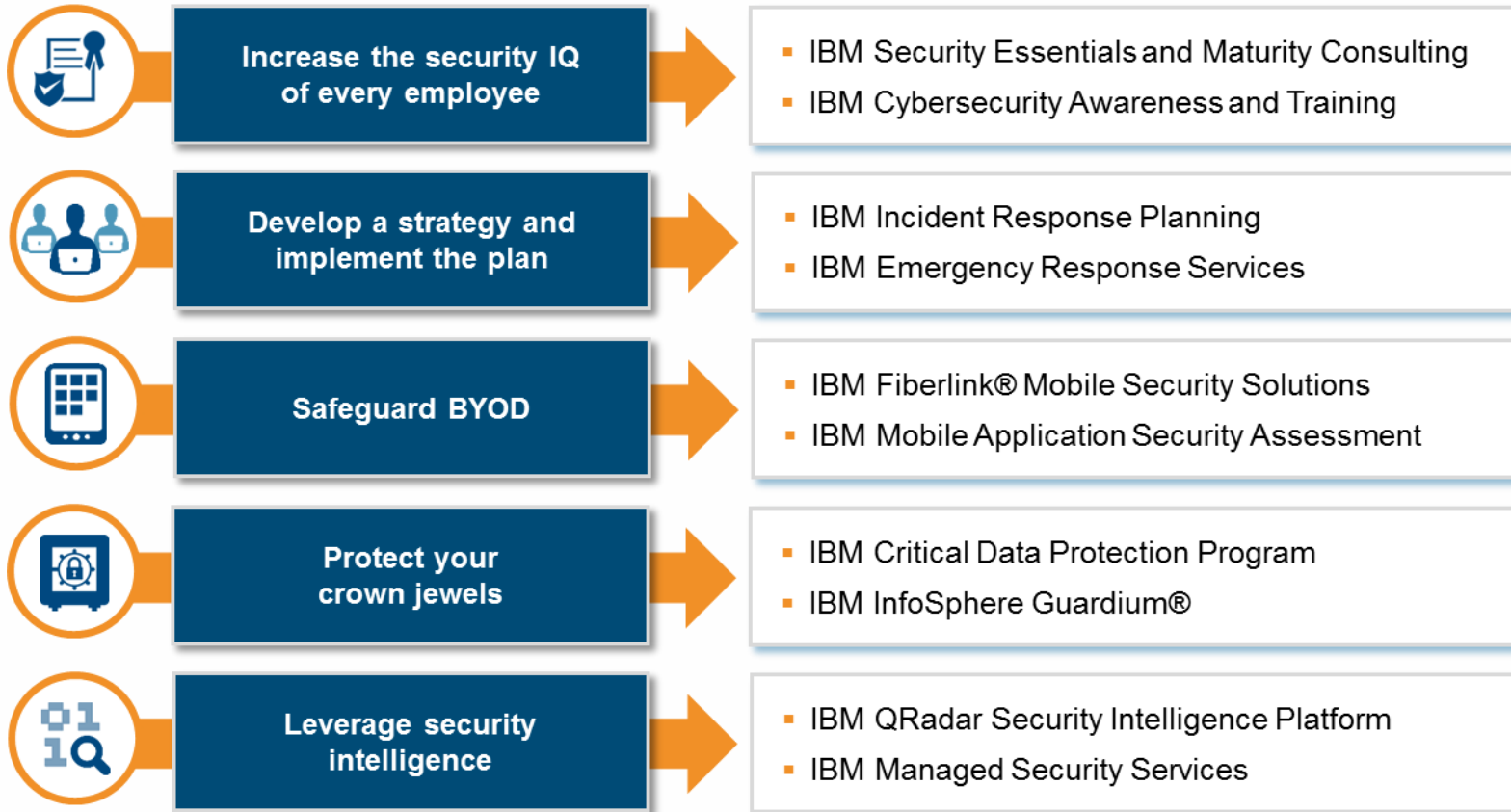
# Use five fundamental security principles to help guide you



# How IBM helps

## What

## How



Security Principles for CEOs

# Cybersecurity is a business risk that you need to manage actively



Get involved. Set the tone and develop a governance model.



Take an active role in policy – even if it's unpopular.



Make security an enabler, not an inhibitor.



Engage the senior leadership.



**Everyone is part of the solution in a risk aware culture,  
and effective security starts at the top**

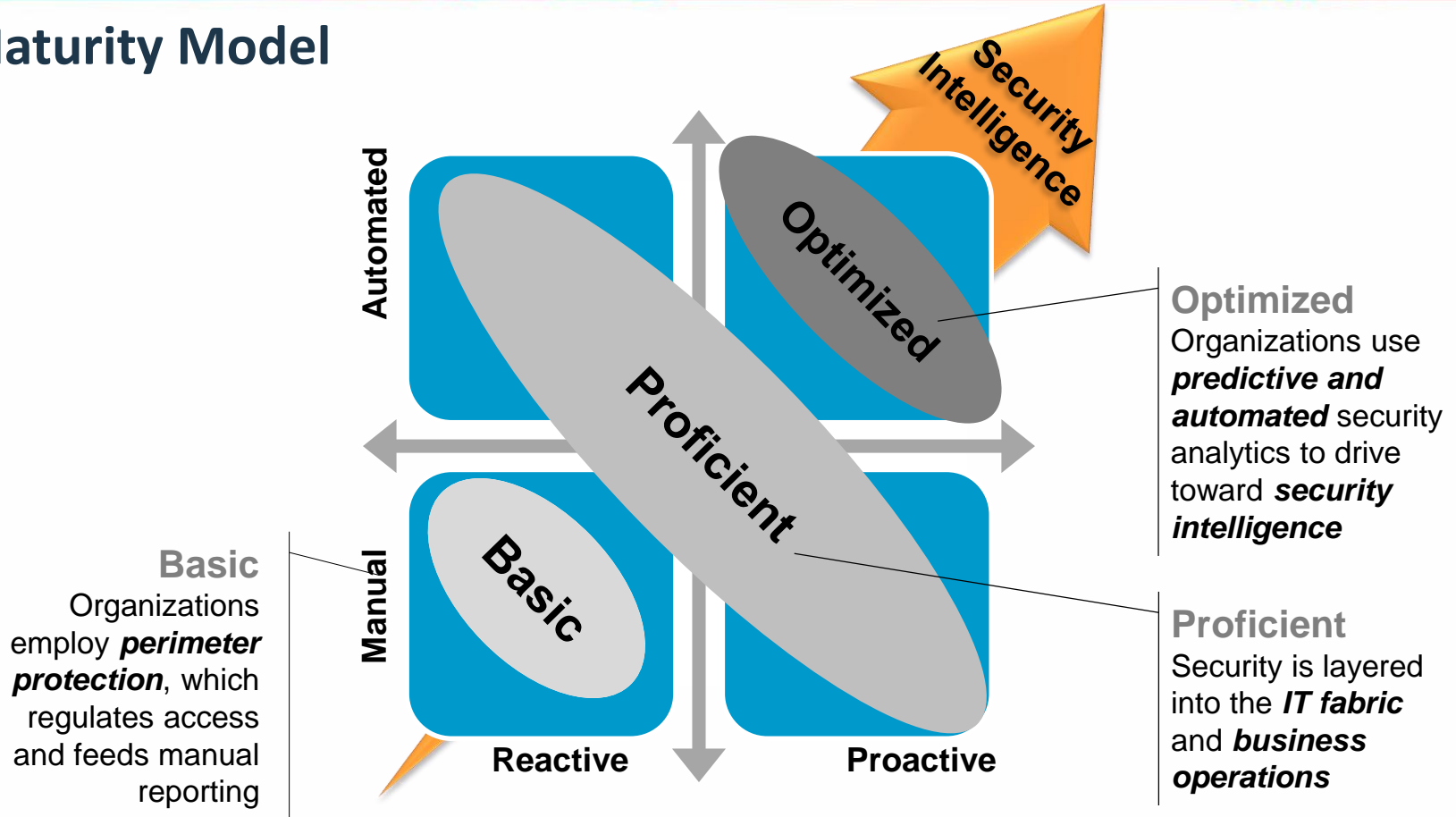




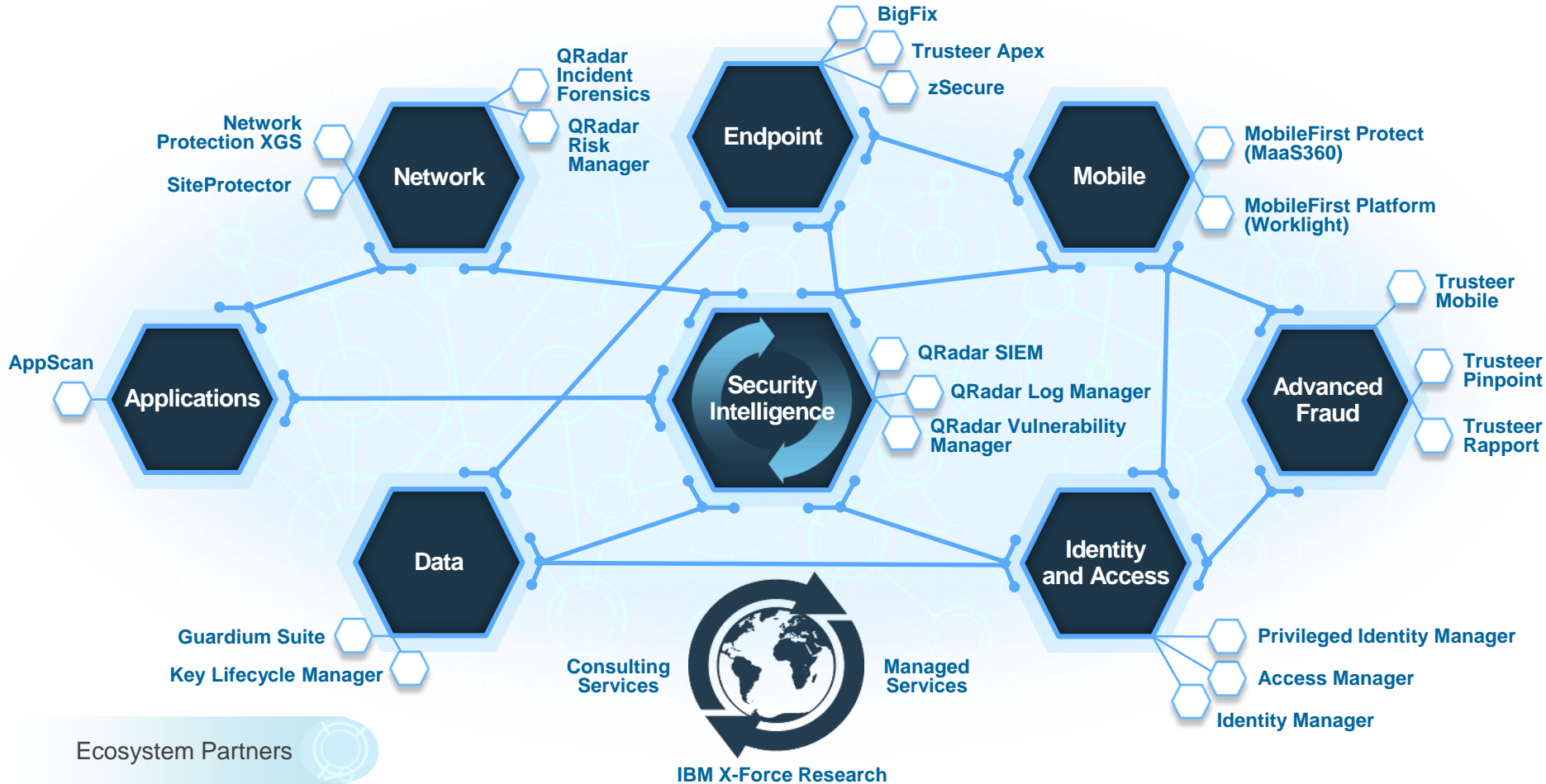
## AGENDA

1. Common Myths
2. Five Fundamentals
3. **Maturity Model**
4. Is My SOC Optimized

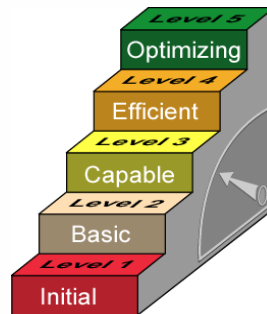
# A Maturity Model



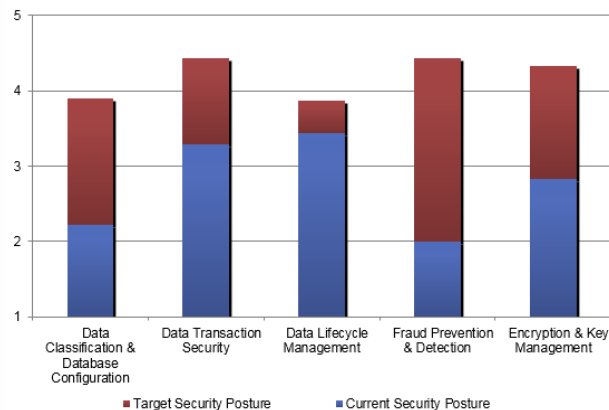
# Remember our Immune System ?



# A Maturity Security Assessment helps you understand your posture and the gap to desired maturity level



Domain	Control	Current Maturity	Gap
Infrastructure	Intrusion Defence and Protection	1	2.6
Advanced Industry Controls	Financial Web Fraud Detection and Prevention	1.63	2.12
Infrastructure	Event Correlation	1.67	2
Application	Secure Coding Practices	2	2.2
Data	Fraud Prevention & Detection	2	2.43
People	Authentication Services & SSO	2	1.88
Infrastructure	Network Security Infrastructure	2.17	1.16
Application	Secure Design & Threat Modelling	2.2	2.2
Data	Data Classification & Database Configuration	2.22	1.67
GRC	Enterprise Security Architecture	2.3	1.8
Application	Application Security Assessment & Testing	2.33	1.5
GRC	Security Risk Management	2.4	1.4
People	Authorization Services	2.44	1.45
Application	Application Inventory	2.5	1.5
Application	Vulnerability Remediation & Risk Mitigation	2.5	1.5
GRC	Information Security Policy	2.6	1.7
GRC	Threat Risk Assessment	2.6	1.4
GRC	Incident Response & Management	2.6	1.4



# Reaching security maturity in context

Security Intelligence and Operations					
Can you identify active attack paths and high-risk assets?					
Can you correlate events across domains and detect advanced threats?					
Are you meeting compliance and reporting requirements?					
	Fraud	Identity	Data	Application	Infrastructure
<b>Optimized</b>	Are your mobile, online and cloud channels secure from cybercrime?	Do you have automated, policy-driven identity and role based management?	Can you monitor (privileged) access to data?	Can you test legacy applications for exposures?	Do you have real-time visibility and full control of your security and operations?
<b>Proficient</b>	Can you identify and stop fraud without negatively impacting user productivity?	How are you managing user access to resources?	Do you know if sensitive data leaves your network?	Are you regularly testing your website for vulnerabilities?	Do you perform proactive threat and vulnerability management protection?
<b>Basic</b>	Are you able to detect and prevent malware and phishing attacks?	Have you rolled out an identity program?	Have you classified and encrypted sensitive data?	Do you have a secure application development process?	Are you providing basic threat management for all endpoints and network devices, including cloud and mobile?

# Reaching security maturity capabilities

Security Intelligence and Operations					
Predictive analytics, big data workbench, flow analytics, forensics					
SIEM and vulnerability management					
Log management					
	Fraud	Identity	Data	Application	Infrastructure
<b>Optimized</b>	<ul style="list-style-type: none"> <li>Transaction protection</li> <li>Endpoint protection</li> </ul>	<ul style="list-style-type: none"> <li>Identity governance</li> <li>Fine-grained entitlements</li> <li>Privileged user management</li> </ul>	<ul style="list-style-type: none"> <li>Data governance</li> <li>Encryption key management</li> </ul>	<ul style="list-style-type: none"> <li>Fraud detection</li> <li>Hybrid scanning and correlation</li> </ul>	<ul style="list-style-type: none"> <li>Multi-faceted network protection</li> <li>Anomaly detection</li> <li>Hardened</li> </ul>
<b>Proficient</b>	<ul style="list-style-type: none"> <li>Login challenge questions</li> </ul>	<ul style="list-style-type: none"> <li>User provisioning</li> <li>Access management</li> <li>Strong authentication</li> </ul>	<ul style="list-style-type: none"> <li>Data masking / redaction</li> <li>Data activity monitoring</li> <li>Data loss prevention</li> </ul>	<ul style="list-style-type: none"> <li>Web application protection</li> <li>Source code scanning</li> </ul>	<ul style="list-style-type: none"> <li>Virtualization security</li> <li>Asset management</li> <li>Endpoint / network security management</li> </ul>
<b>Basic</b>	<ul style="list-style-type: none"> <li>Device ID rules</li> </ul>	<ul style="list-style-type: none"> <li>Directory management</li> </ul>	<ul style="list-style-type: none"> <li>Encryption</li> <li>Database access control</li> </ul>	<ul style="list-style-type: none"> <li>Application scanning</li> </ul>	<ul style="list-style-type: none"> <li>Perimeter security</li> <li>Host security</li> <li>Anti-virus</li> </ul>

# IBM Security Product Portfolio

## IBM Security Product Portfolio

### Security Intelligence and Analytics

QRadar Log Manager		QRadar Security Intelligence		QRadar Risk Manager		QRadar Vulnerability Manager		QRadar Incident Forensics	
Fraud		Identity		Data		Application		Infrastructure	
Trusteer Fraud Protection Suite		Identity Governance		Guardium Activity Monitoring for Databases		AppScan Source		Next Generation Network Protection (XGS)	
Trusteer Pinpoint Detect		Identity Manager		Guardium Activity Monitoring for Files		AppScan Standard		SiteProtector <i>(threat management)</i>	
Trusteer Pinpoint Malware Detection		Privileged Identity Manager		Guardium Data Encryption		AppScan Enterprise		Trusteer Apex	
Trusteer Rapport		Access Manager		Optim Data Privacy		DataPower Web Security Gateway		IBM BigFix	
Trusteer Mobile SDK and Secure Browser		Directory Suite		Key Lifecycle Manager		Security Policy Manager		IBM MaaS360	
								IBM Cloud Security Enforcer	
								zSecure	

IBM X-Force Research



## AGENDA

1. Common Myths
2. Five Fundamentals
3. Maturity Model
4. Is My SOC Optimized ?



# Security Operation Center (SOC)



# Why a SOC ?

*Reduce enterprise risk. **Protect** the business.*

*Move from reactive response to **proactive** mitigation.*

*Increase **visibility** over the environment.*

*Meet **compliance**/regulatory requirements.*

*Find bad things and make them go away !*



# Cyber Security Command Centre (CSCC)

Strategy

**Cyber-Security Command Center (CSCC)**  
 Governance / Collaboration / Requirements / Briefings

Operations

**Service Delivery & Operations Management**  
 Service Level Management / Efficiency / Capacity Management / Escalation

**Security Analytics & Incident Reporting**

**Architecture & Projects**

**Administration & Engineering**  
 Rule Dev/Tuning  
 Tool Integration  
 Device Mgmt

**Security Intelligence**

Intel Analysis

Use Case Mgmt

IOC Management

Runbook Mgmt

Active Defense

Threat Hunting

**Security Integration**  
 Vulnerability Mgmt  
 Identity-Access Mgmt,  
 Data Security,  
 Cloud Computing

**CSIRT**  
 Emergency Response  
 Forensic Handling

**Tier 1 Monitoring** ↔ **Tier 2 Triage** ↔ **Tier 3 Response** ↔ **CSIRT**

**Corporate Operations**

- Business Units
- Risk Management
- Audit / Compliance
- Legal / Fraud
- PR / Communications

**IT/OT Operations**

- Help Desk (ITSM)
- Network Operations
- Server Admin (OS,DB,etc.)
- Development
- Physical Security

Technology

**Platforms and Data Components**

SIEM

Ticketing & Workflow

Reporting & Dashboards

Big Data

Intelligence

Active Defense

<b>Data Sources</b>	<b>Intelligence Sources</b>	<b>Business Intelligence</b>	<b>Asset Information</b>
Structured (transactional) Referential Data Sets (integrated) Unstructured (big data)	Subscriptions (vendor/associations) Open Source (social/news/blogs) Private (trust groups/government)	Structure & Geography Data Classification Risk/Impact Analysis	Inventory / CMDB Vulnerability Data Network Hierarchy

**Legend**

- SOC
- IT / OT
- Corporate

# SOC reporting provide insight

## Security Operations Centre Executive Dashboard

August 14 - August 20th 2013

**Security Operations Centre Status Summary**

Overall SOC Security Risk Rating ●

SOC Threat Detection ●

SOC Threat Response Rating ●

**Legend**

KPI within target range ● Improving ↕

KPI >10% from target ● Declining ↘

KPI >25% from target ● No Change ↔

**Weekly Highlights**

Data leak discovered, proprietary RBC data was sent outside the bank. The data was recovered, the external site blocked and contractor responsible was identified. The contractor's access was cut-off and Security was notified to escort the contractor from the premises.

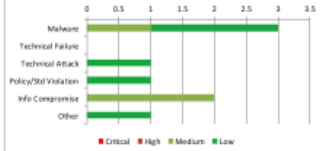
Threats detected last 7 days 106



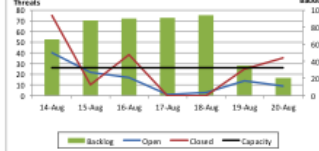
Threat responses last 7 days 180



Severity of Incidents by Category

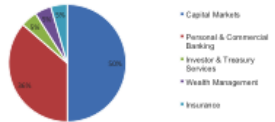


SOC Threat Workload (Last 7 Days)

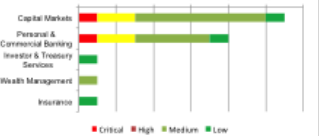


Threats by Business Unit, Geography, Function <DRAFT DATA>

Percentage of Threats by BU



Severity of Incidents by BU



Weekly SOC Operations Activity Summary

Activity Description	Total
Threats/Incidents Closed (All Teams)	182
Incidents Opened (CSIRT Team)	15
Potential Incidents (Threat Stage Team)	22
Qualified Threats (Abolishing Team)	100
Potential Threats (Quadrant Officers)	80
Log Events Passed by Onadar	10,635,945,588

Weekly SOC Operations Key Performance Indicators

Description	Target*	Actual	Delta	Delta%
Process Cycle Efficiency	40.0%	7.9%	-32.1%	-80%
Process Capability	TBD	TBD	TBD	TBD
Average Cost per Threat	TBD	TBD	TBD	TBD
Staff Utilization	TBD	TBD	TBD	TBD
Work in Process (Incidents)	200	34	-166	-83%
Backlog Tickets	100	50	-50	-50%
Average Response Time (Hrs)	12.0	12.0	0.0	0%
Average Handling Time (Hrs)	1.0	1.1	0.1	10%
Average Cycle Time (Days)	2.5	3.5	1	40%
-Critical	0 incidents	0.3	0	0%
-High	0 incidents	1.0	5.0	400%
-Medium	3 incidents	3.0	0	0%
-Low	5 incidents	5.0	0	-60%

\*Note: Targets are preliminary and will be based on the next 90 days as the SOC reaches Steady State

## Security Operations Centre Daily Flash Report

August 6th 2013

**Daily highlights:**

No new major threats detected, high priority threats have been identified, evaluated, mitigated and remediated  
 SOC threat detection operating normally, log processing, rules active, staffing adequate, no issues  
 Small backlog of medium and low priority threats, working to increase efficiency and throughput as staff gain experience

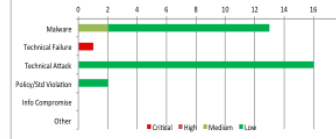
Threats detected yesterday 158



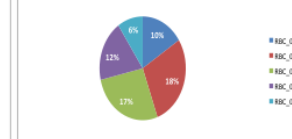
Threat responses yesterday 128



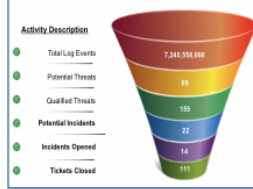
Severity of Incidents by Threat Category (Yesterday)



Source of Threats % by Offense (Yesterday)



24 hour SOC Activity



Key Performance Indicators

Work in Progress	63
Avg Response Time	12 hours
Avg Ticket Handle Time	24 hours

Description	Open	Target	Delta	Age (Days)	Target (Days)	Delta (%)
Work in Progress Security Tickets	63	25	-38	11	11	0%
Work in Progress Non-Security Tickets	0/0	0/0	0/0	0/0	0/0	0%

Weekly SOC Operations Key Performance Indicators

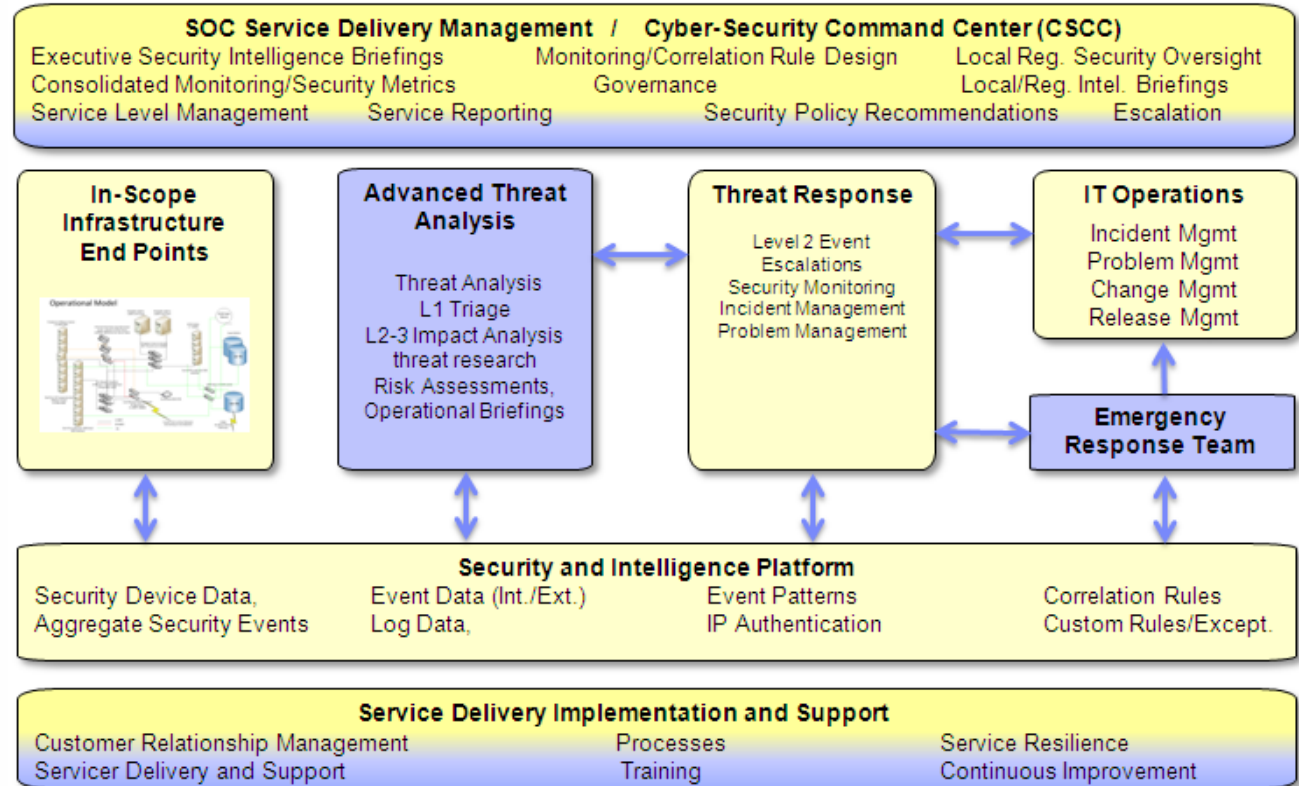
Description	Target*	Actual	Delta	Delta%
Process Cycle Efficiency				
Process Capability				
Average Cost per Threat				
Staff Utilization				
Work in Process (Incidents)	200	34	-166	-83%
Backlog Tickets	100	50	-50	-50%
Average Response Time (Hrs)	12.0	12.0	0.0	0%
Average Handling Time (Hrs)	1.0	1.5	0.5	50%
Average Cycle Time (Days)	2.5	3.5	1	40%
-Critical	0 incidents	0.3	0.7	0.36
-High	0 incidents	1.0	5.0	4
-Medium	0 incidents	3.0	3.0	0
-Low	0 incidents	5.0	2.0	-3

\*Note: Targets are preliminary and will be based on the next 90 days as the SOC reaches Steady State

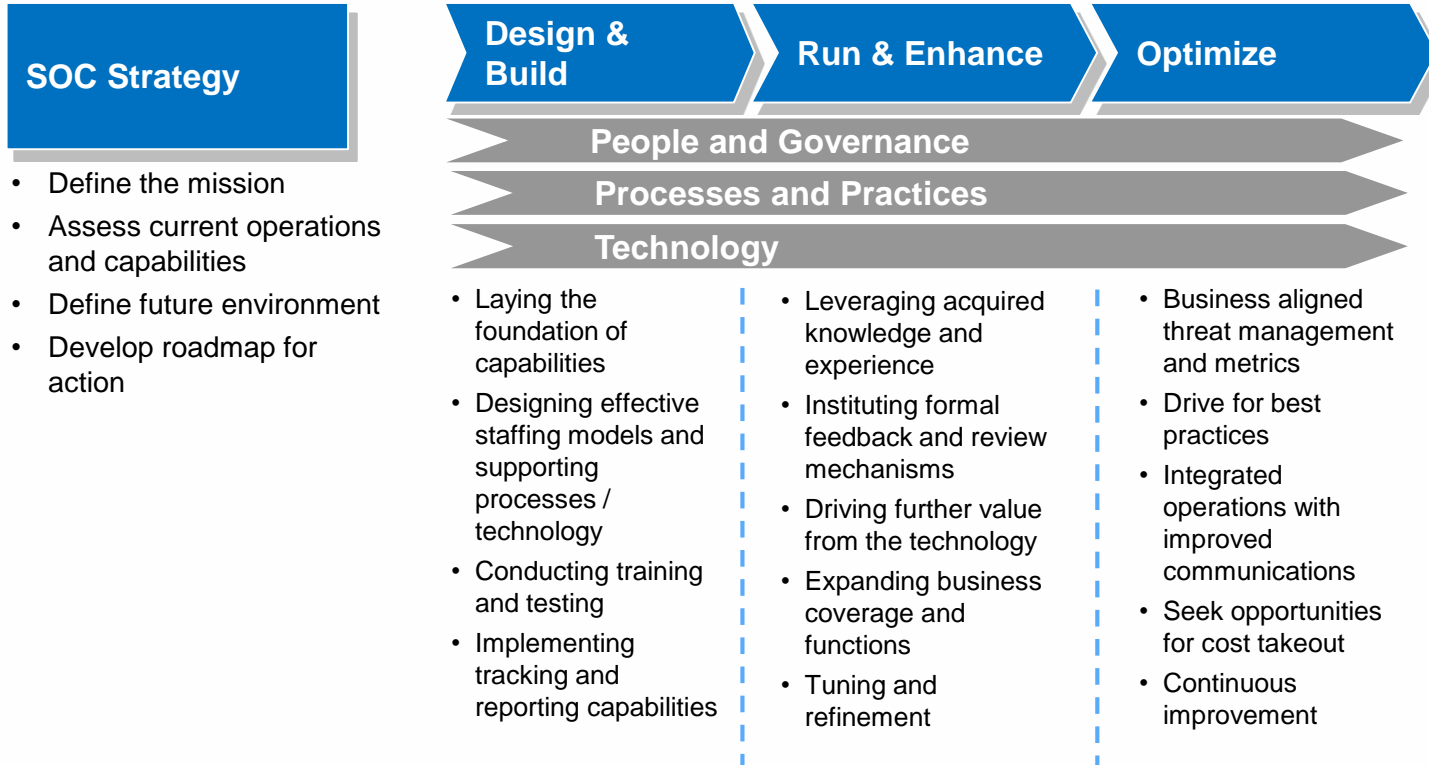
# Hybrid SOC Model : improved technical capabilities with low cost of service

## Advantages:

- Client retains program control
- Highly scalable
- Adapts to changes
- Minimal complexity
- Leverage best practices
- Access to industry leading security intelligence
- Skills transfer
- Quick startup ~90 days
- Minimizes operating costs



# IBM proposes a phased approach to build a SOC



# IBM SOC Consulting is an integral part of our Security Services



## Strategy and assessment

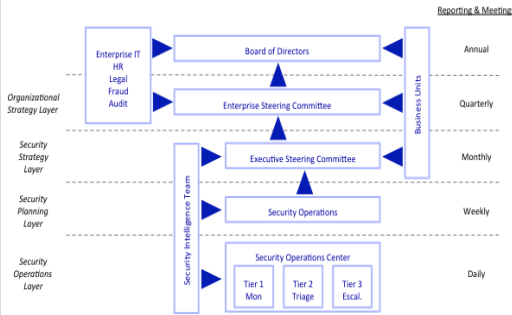
- Consulting services to help a client assess their current security operations, identify gaps that impede rapid remediation of threats, and develop a strategy for designing and building a best-of-breed security operations center (SOC)

## Design and deployment

- Consulting and implementation services to help a client design and build a single or multiple security operations centers (SOC's) that will provide the security intelligence and management capabilities to better understand the threats and their impact on the organization and ensure that the infrastructure is at a state of continual readiness to prevent malware from causing data loss or impacting productivity
- Deployment services to implement, configure, and test leading SIEM technologies

# Security program must leverage industry best-practices to rapidly deploy SOC capabilities.

## Program Governance



## Organizational RACI

	SOC Analyst Monitoring	SOC Analyst Triage	SOC Analyst Response	Security Intelligence Analyst	Security Incident Analyst (On/Off)	SOC Manager	SOC Admin	Security Process Analyst	IT Security Admin	Operations	CSIRT
<b>Core Security Services</b>											
Security Monitoring	A	C									
Incident Triage	C	A	C								
Incident Response	C	A	C	A							
Delivery Management	C	A	C	A							
<b>Deployment Services</b>											
Use Case Design	C	C	C	C	A						
Security Testing & Tuning	A	C									
Security Process Development	C	C	C	A							
Security Training	C	C	C	A							
Security Intelligence Briefings	C	C	C	A							
Security Intelligence Analysis	C	C	C	A							
<b>Administrative Services</b>											
SIEM Administration	C										
Log Source Management	C										
Log Source Health & Monitoring	C										
<b>Reporting Services</b>											
Security Reporting	C	C	C	C	A						
Efficiency Reporting	C	C	C	C	A						
Financial Reporting	C	C	C	C	A						
<b>Optional Services</b>											
Enterprise Incident Management	C	C	C	C	A						
Forensic Investigation	C	C	C	C	A						
Policy Violation Handling	C	C	C	C	A						

## Security Analytics & Dashboards

### Security Operations Center (SOC) - (Frequency) Report

Reporting Period: DD-MMMM-YYYY to DD-MMMM-YYYY

**Thwarted REALLY BAD threat - 319 systems patched ahead of exploit. No Client systems compromised.**

**Identification** (Yellow) **Mitigation** (Green) **Remediation** (Red)

IT Admin resources in Business Unit ABC have been redirected to project work, limiting

**REMEDIAL BUSINESS AREA: DATA CENTER**

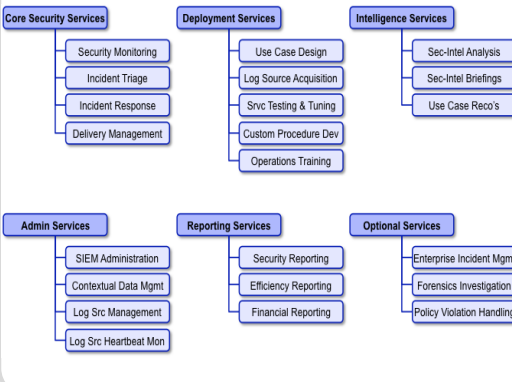
Category	Count	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Phase 8
IT Security	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC1)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC2)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC3)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC4)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC5)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC6)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC7)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC8)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC9)	10	10	0	0	0	0	0	0	0
IT Security (Data Center - DC10)	10	10	0	0	0	0	0	0	0

**MATURITY TREND LAST 4 QUARTERS**

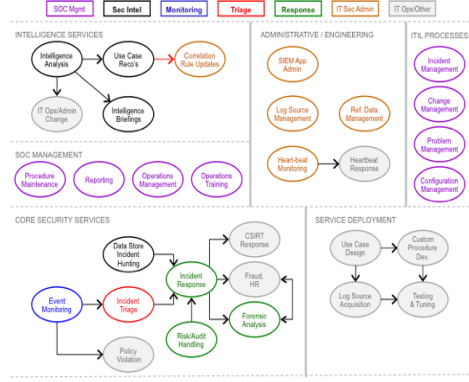
**Workload & Capacity Tier 1 - Triage**

**Workload & Capacity Tier 2 - Response**

## Security Operations Service Catalog



## Optimized Processes & Tailored Runbooks



**Security Incident Post Mortem**

Average Incident Resolution Phase

Incident	Description	Phase 1 Result	Phase 2 Mitigation	Phase 3 Contain	Phase 4 Eradicate	Phase 5 Recover	Phase 6 Restore	Phase 7 Lessons & Recommendations
SOC-001234	CERTFICAL - exec laptop/module compromise	Success	Success	Success	Success	Success	Success	10/12: Laptop was reimaged
SOC-001235	W008 - AP middleware servers exploit	Success	Success	Success	Success	Success	Success	10/12: patches scheduled for deployment during next maintenance window (10/24)
SOC-001236	CERTFICAL - crown jewel application server	Success	Success	Success	Success	Success	Success	Attack bypassed control / Attack mitigated by control

**Workload Analysis**

**Workload & Capacity Tier 1 - Triage**

**Workload & Capacity Tier 2 - Response**

**Threats by Priority**

**Threats by Category**



# Case Study: A major European bank with global compliance challenges

## Business Challenge:

A large European bank was searching for best practices and assistance in creating an in-house, Security Operations Center.

## Solution:

IBM performed a security operations maturity assessment.

Benchmarked the client's capabilities against peers

Assessed the maturity across multiple dimensions

Projected their desired state by end of year 1 and 3

Created of a roadmap that focused priority areas



## Business Benefits:

- Insight into the relative maturity of the security operations
- An ability to identify and prioritize development activities
- A view on how they could better leverage internal resources and security intelligence to improve risk posture





# THANK YOU








[www.ibm.com/security](http://www.ibm.com/security)

# Backup

# Where should customers turn?

## Security Intelligence and Vulnerability Management

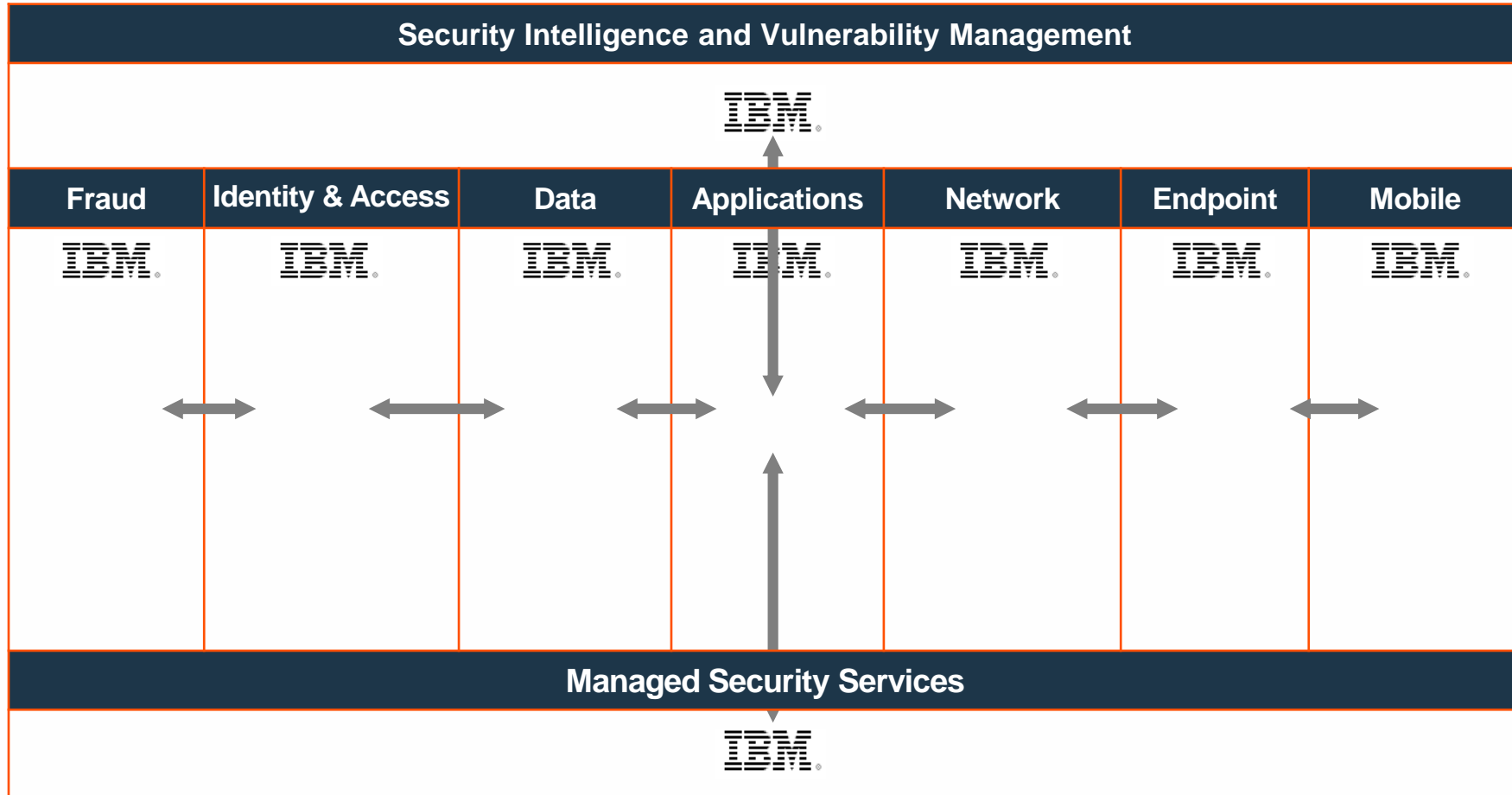
- AccessData
- Akamai
- Alien Vault
- BlueCoat
- EMC
- Guidance Software
- Hewlett-Packard
- Intel Security
- LogRhythm
- IBM
- NetIQ
- NIKSUN
- Prolexic
- Qualys
- Rapid7
- Splunk
- Symantec
- Tripwire
- Tenable Network Security
- Vigilant

Fraud	Identity & Access	Data	Applications	Network	Endpoint	Mobile
 <ul style="list-style-type: none"> <li>• 41st Parameter</li> <li>• Accertify</li> <li>• EMC</li> <li>• Guardian Analytics</li> <li>• iovation</li> <li>• NICE Systems</li> <li>• ThreatMetrix</li> </ul>	 <ul style="list-style-type: none"> <li>• CA Technologies</li> <li>• Dell</li> <li>• EMC</li> <li>• Entrust</li> <li>• Okta</li> <li>• OneLogin</li> <li>• Oracle</li> <li>• PingIdentity</li> <li>• Symantec</li> </ul>	 <ul style="list-style-type: none"> <li>• EMC</li> <li>• Entrust</li> <li>• Imperva</li> <li>• Intel Security</li> <li>• SafeNet</li> <li>• Symantec</li> <li>• Verdasys</li> <li>• Vormetric</li> </ul>	 <ul style="list-style-type: none"> <li>• Appthority</li> <li>• F5 Networks</li> <li>• Hewlett-Packard</li> <li>• Qualys</li> <li>• Trustwave</li> <li>• Veracode</li> <li>• WhiteHat Security</li> </ul>	 <ul style="list-style-type: none"> <li>• Arbor</li> <li>• CheckPoint</li> <li>• Cisco</li> <li>• Dell</li> <li>• FireEye</li> <li>• Fortinet</li> <li>• Hewlett-Packard</li> <li>• Intel Security</li> <li>• Juniper</li> <li>• Palo Alto Networks</li> <li>• Sourcefire</li> </ul>	 <ul style="list-style-type: none"> <li>• ESET</li> <li>• F-Secure</li> <li>• Intel Security</li> <li>• Kaspersky</li> <li>• Lumension</li> <li>• Microsoft</li> <li>• Sophos</li> <li>• Symantec</li> <li>• Trend Micro</li> </ul>	 <ul style="list-style-type: none"> <li>• Good</li> <li>• Check Point</li> <li>• Cisco</li> <li>• Citrix</li> <li>• Intel Security</li> <li>• Microsoft</li> <li>• MobileIron</li> <li>• Sophos</li> <li>• Symantec</li> <li>• VMware</li> <li>• Webroot</li> <li>• Zscaler</li> </ul>

## Managed Security Services

- Dell
- HP
- IBM
- Symantec
- Verizon

# Where should customers turn?



# IBM Security latest analyst report rankings

Domain	Market Segment / Report	Gartner	Forrester	IDC
<b>Security Intelligence</b>	Security Information and Event Management (SIEM)	LEADER		LEADER
<b>Fraud Protection</b>	Web Fraud Detection (Trusteer)	LEADER		
<b>Identity and Access Management</b>	Federated Identity Management and Single Sign-On			LEADER
	Identity and Access Governance	LEADER	Strong Contender	
	Identity and Access Management as a Service (IDaaS)	Visionary		
	Web Access Management (WAM)	LEADER		
	Mobile Access Management	LEADER <i>Frost &amp; Sullivan</i>		
	Identity Provisioning Management	LEADER <i>KuppingerCole</i>		
<b>Data Security</b>	Data Masking	LEADER		
<b>Application Security</b>	Application Security Testing (dynamic and static)	LEADER	LEADER	LEADER
<b>Network, Endpoint and Mobile Security</b>	Intrusion Prevention Systems (IPS)	LEADER		
	Endpoint: Client Management Tools	LEADER		
	Endpoint Protection Platforms (EPP)	Niche	Strong Performer	
	Enterprise Mobility Management: MobileFirst Protect (MaaS360)	LEADER	LEADER	LEADER
<b>Consulting and Managed Services</b>	Managed Security Services (MSS)	LEADER	LEADER	LEADER
	Information Security Consulting Services		LEADER	

Note: Rankings compiled as of February, 2016

■ No ranking available

V2016-02-15

# IBM Security Portfolio

SECURITY  
TRENDS



Advanced  
Threats



Cloud



Mobile and  
Internet of Things



Compliance  
Mandates



Skills  
Shortage

## IBM Security Capability Framework

Strategy, Risk and Compliance

Cybersecurity Assessment and Response

Security Intelligence and Operations

Advanced Fraud  
Protection

Identity and Access  
Management

Data  
Security

Application  
Security

Network, Mobile and  
Endpoint Protection

*Advanced Threat and Security Research*

DELIVERY  
MODELS

Management  
Consulting

Systems  
Integration

Integrated  
Products

Security-  
as-a-Service

Managed  
Security

Partner  
Ecosystem