

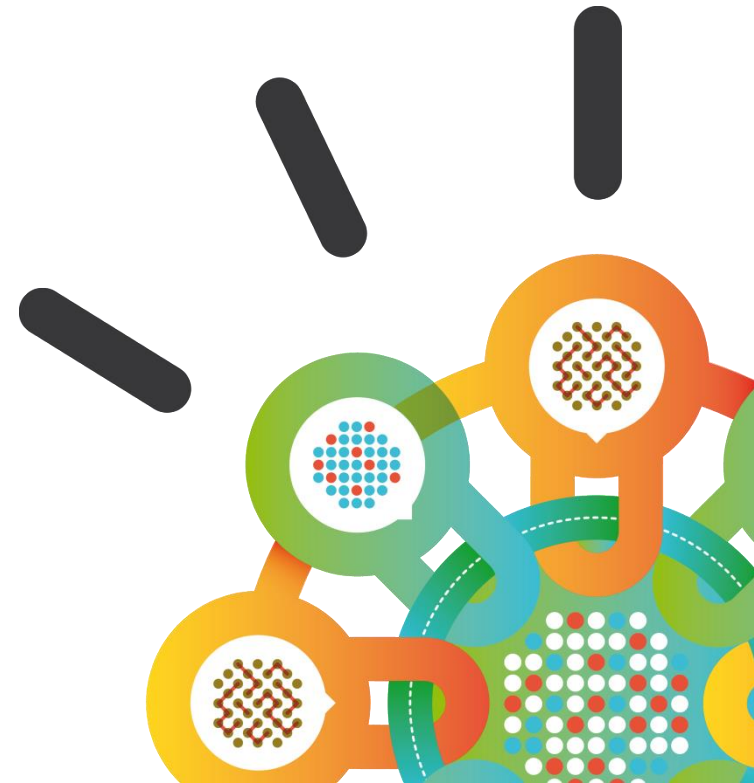
Security Intelligence.
Think Integrated.

IBM Security

Taking a Hybrid IT Approach to Solving Today's Top Security Challenges

Speaker: Mike Monticello
IBM Security Intelligence Director

May 19, 2015





IBM X-Force

is the foundation for advanced security and threat research across the IBM Security Framework.

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

IBM X-Force monitors and analyzes the changing threat landscape

Coverage

20,000+ devices
under contract

15B+ events
managed per day

133 monitored
countries (MSS)

3,000+ security
related patents

270M+ endpoints
reporting malware



Depth

25B+ analyzed
web pages and images

12M+ spam and
phishing attacks daily

96K+ documented
vulnerabilities

860K+ malicious
IP addresses

Millions of unique
malware samples

83% of CISOs say that the challenge posed by external threats has increased in the last three years

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

800,000,000+ records were leaked, while the future shows no sign of change

“Insane” Amounts of Records Breached

42% of CISOs claim the risk from external threats increased dramatically from prior years.

2012

2013

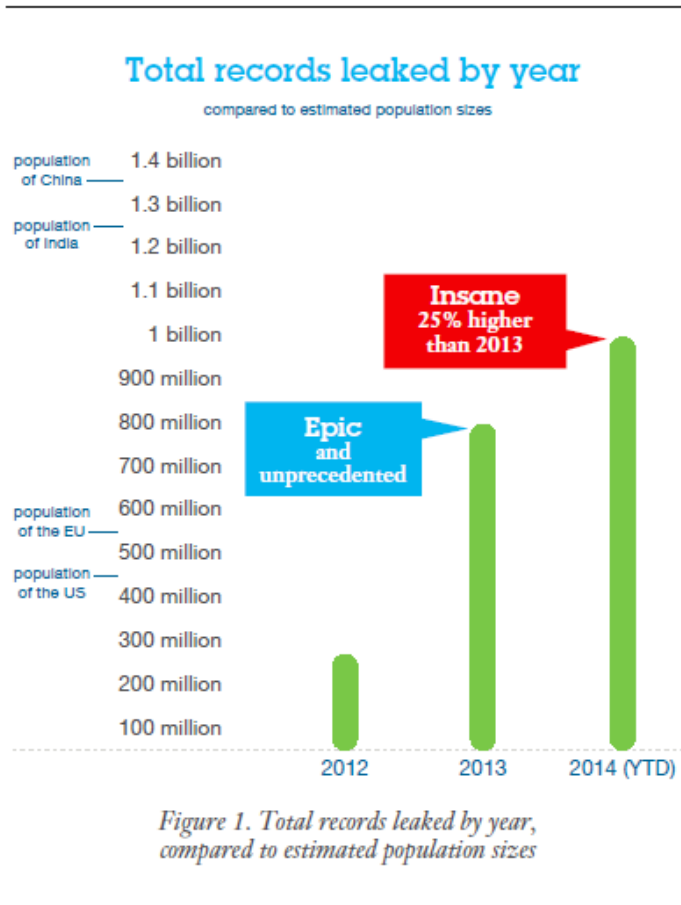
2014



Size of circle estimates relative impact of incident in terms of cost to business.

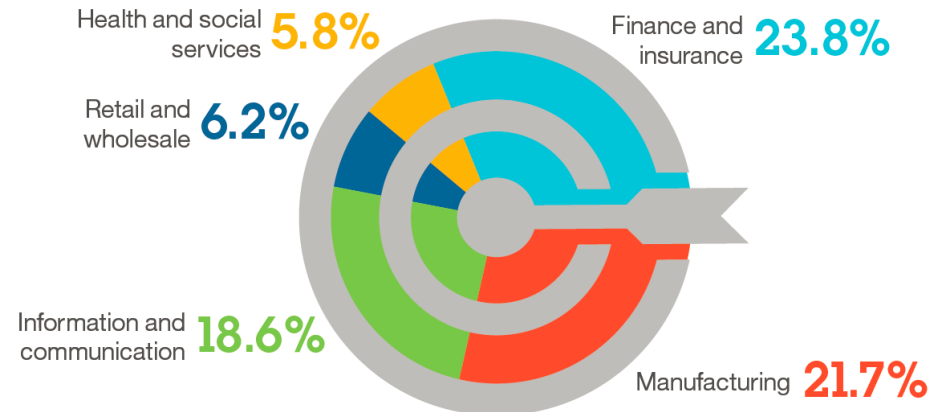
A historical look at security incidents by attack type, time and impact, 2012 through 2014

Sophisticated attackers break through safeguards every day

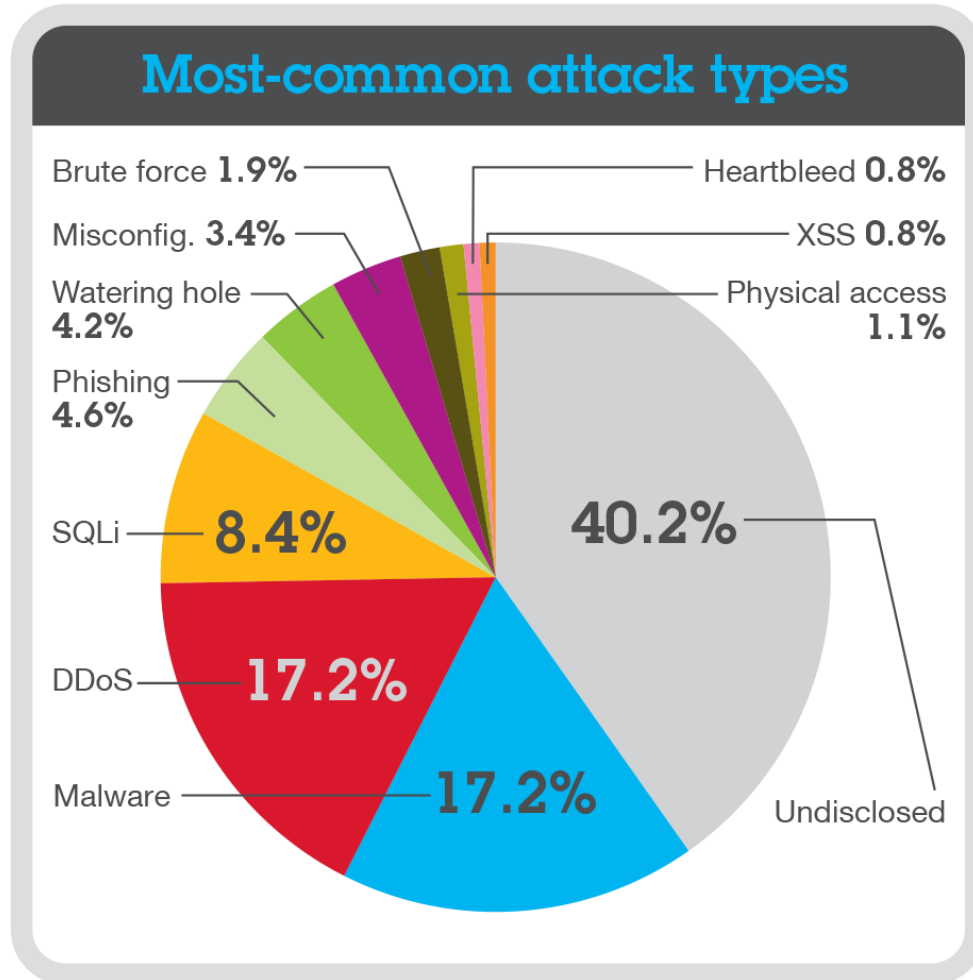


Incident rates across monitored industries


Over 75% of incidents targeted 5 industries




Attackers are applying fundamental attack types in creative, new ways; altering the threat landscape




The soaring impact of breaches has created a new security reality



3X
increase in Java
vulnerabilities¹



\$ 15%
increase in
cost of a breach²



More Risk and Bigger Impact

500,000,000
records breached³



\$3.5M
average cost / breach²

1) Q3 2014 IBM X-Force Research and Development, increase from 2012 to 2013

2) 2014 Cost of a Data Breach, Ponemon Institute, global average cost, 15% increase from 2012 to 2013

3) Q3 2014 IBM X-Force Report

The tone of breaches has shifted, revealing disturbing flaws in the fundamentals of both systems and security practices

A lack of security fundamentals

- End-user password re-use
- Leaving default passwords on admin systems
- Poor challenge questions for password reset procedures

Cracks in the foundation

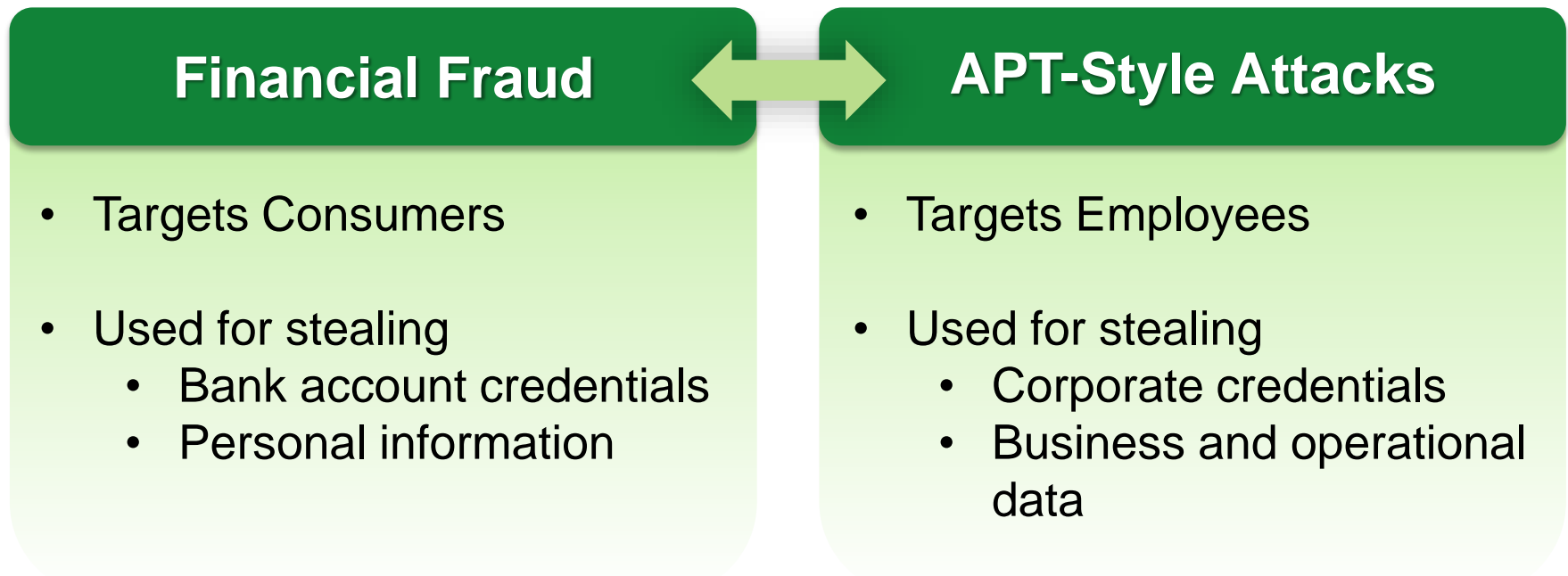
- The same operating systems, open-source libraries and CMS software are prevalent on many websites
- Several of these systems and libraries had vulnerabilities disclosed in 2014

Shrinking privacy in a digital world

- Sensitive photos stored on a cloud service were leaked due to weak passwords
- Private email communications at a major Hollywood studio were released

59% of CISOs strongly agree the sophistication of attackers is outstripping the sophistication of their organization's defenses

Particularly troubling is the adaptation of malware toolkits from targeting financial institutions to APT-style attacks on a broader range of industries



Massively distributed APT malware is being used to target industries beyond traditional financial targets

Massively Distributed

- Off the shelf malware, not custom designed
- Using mass distribution campaigns
- Millions of machines already infected!

Comprehensive Menu of Advanced Capabilities

- Keylogging and screen capturing
- Remote code execution
- Full remote control

Able to be Repurposed

- Communicates with a C&C
- Receives operational instructions via config file
- Config file can be updated with new operational instructions

Highly Evasive

- Sophisticated evasion techniques used to bypass detection
- Can remain stealthy on the machine for lengthy periods of time

Citadel is available for sale on the Russian underground, with new features prioritized by crowdsourcing to target new industries



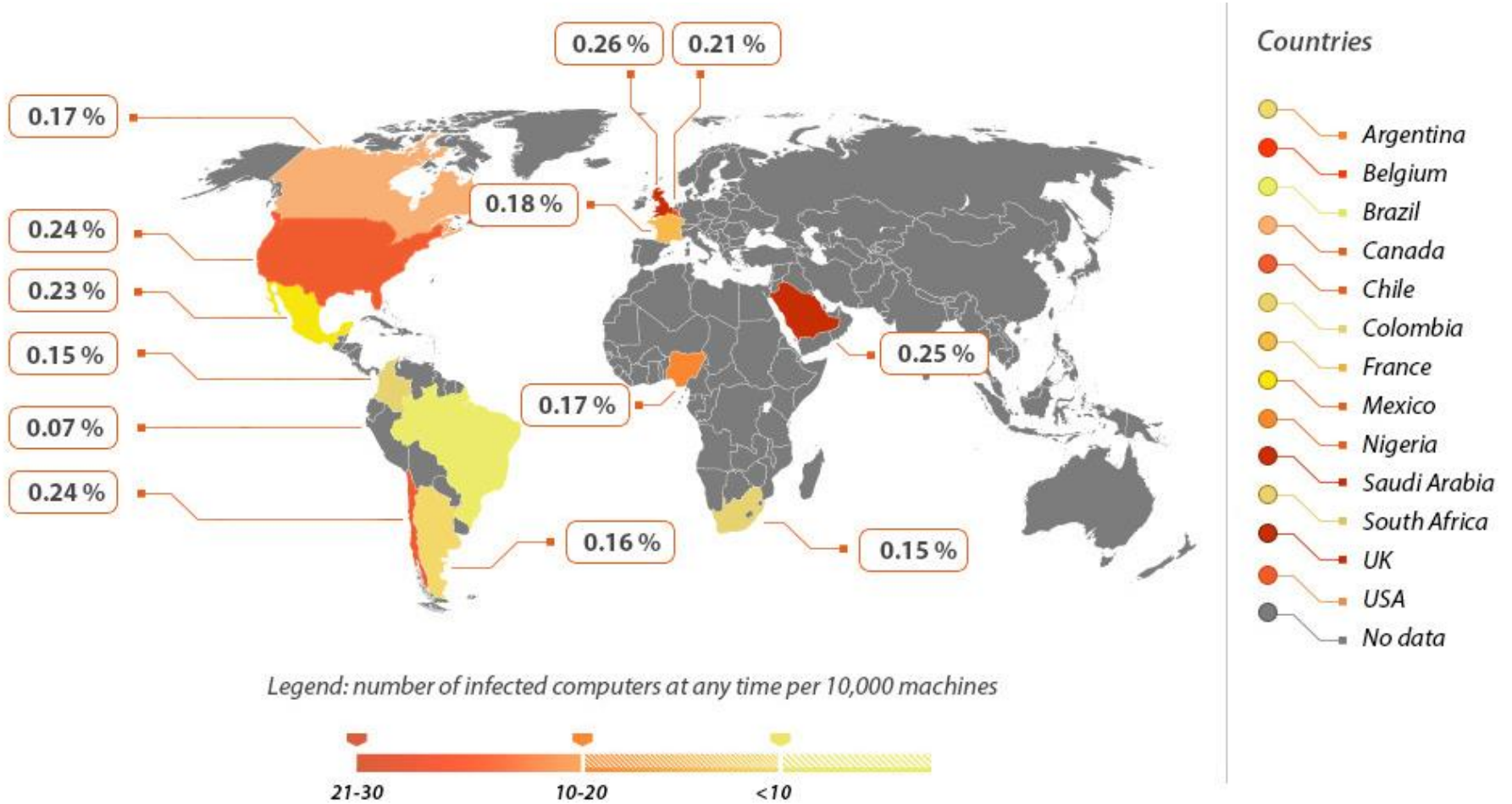
Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical Organizations



Cybercriminals Use Citadel to Compromise Password Management and Authentication Solutions

An average of 1 in 500 machines is infected with a Mad APT at any point in time

Infection Rates for Massively Distributed APT Malware by Country



Since traditional security isn't effective against Mad APTs, what can you do to mitigate these types of threats?

Employee endpoint protection

Cloud based malware detection

Advanced malware detection and robust security intelligence

Emergency response plans and practice

IBM Security Portfolio

SECURITY
TRENDS

 Advanced
Threats

 Cloud

 Mobile and
Internet of Things

 Compliance
Mandates

 Skills
Shortage

IBM Security Portfolio

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

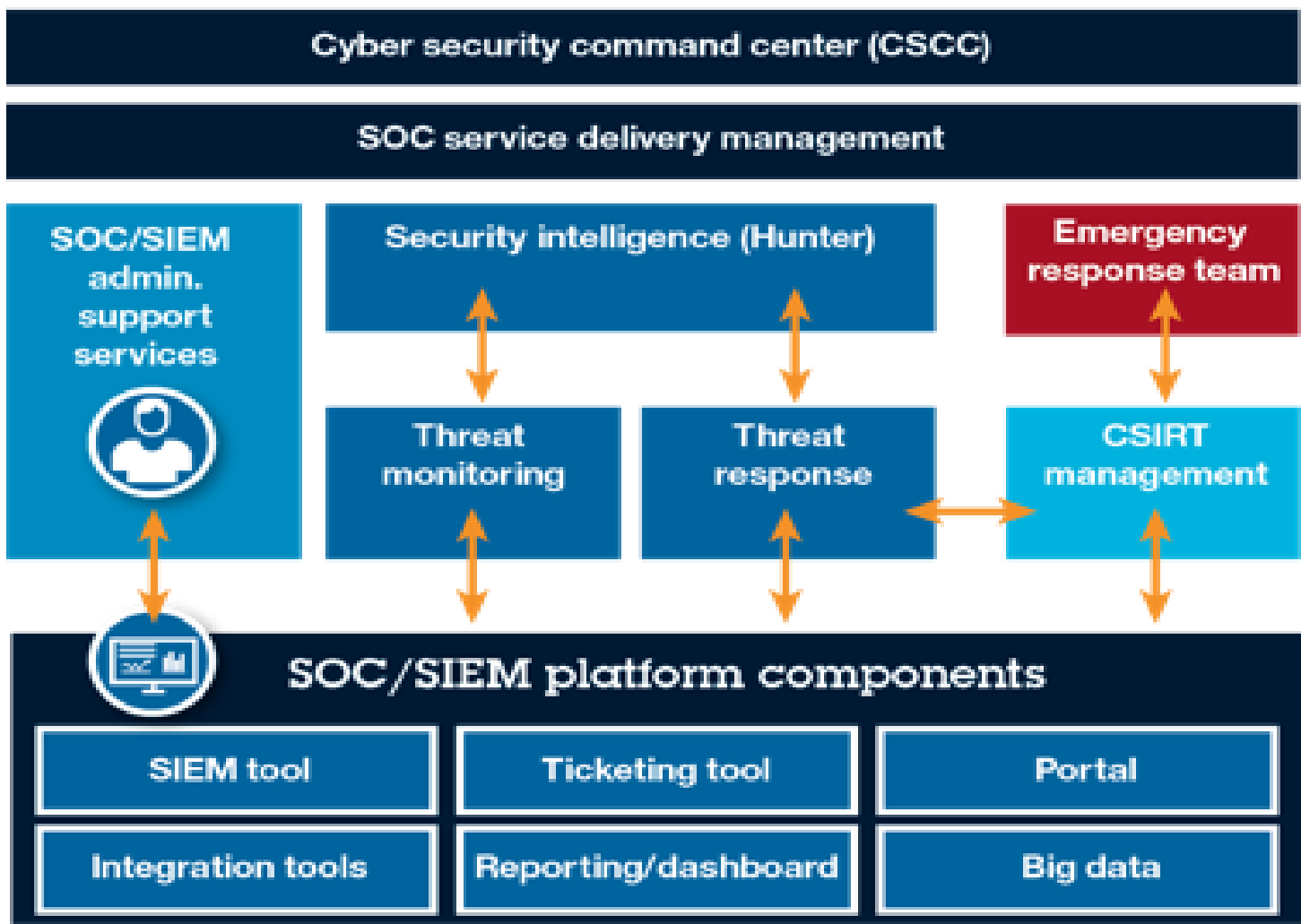
Partner
Ecosystem

The top challenges of enterprise security



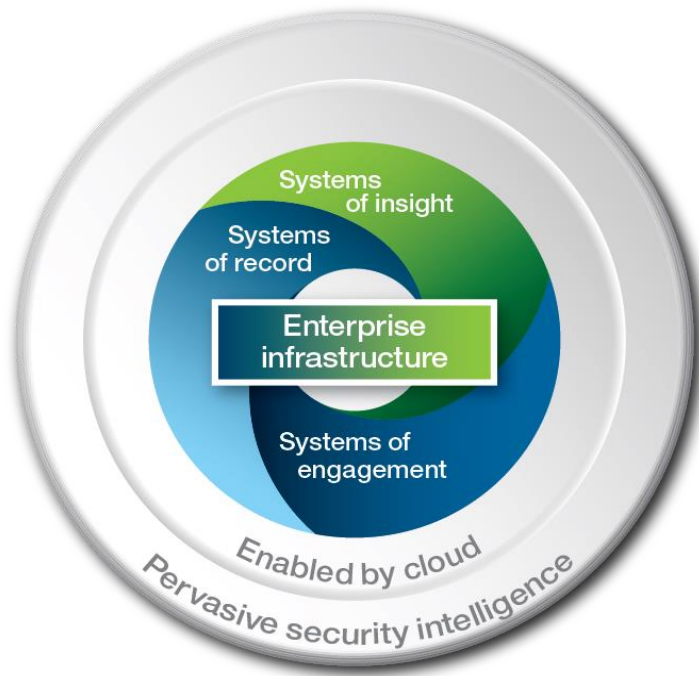
- Growing number of attacks
- Single threaded threat response
- Ongoing skills shortage
- Administrative complexity
- Increased flexibility

Security leaders must adopt a more transformational approach to SOC design and administration



Staking IBM's claim for differentiated value

Enterprise Hybrid IT



When systems of record...Fuse with systems of engagement....To create systems of insight

Enterprise Hybrid IT is...

“Equipping an enterprise to meet – and exceed – the rising expectations of every customer by purposefully fusing and securing established and emerging technology and services.”

Enterprise Hybrid IT enables companies to achieve competitive advantage by:

- Innovating business models, products and services at speed, and at scale....securely
- Using data to make better business decisions and drive revenue
- Establishing a holistic view of technology needs
- Maximizing the return on existing investments
- Quickly adopting and applying new technology

The evolution of managed security services to support and secure hybrid IT environments

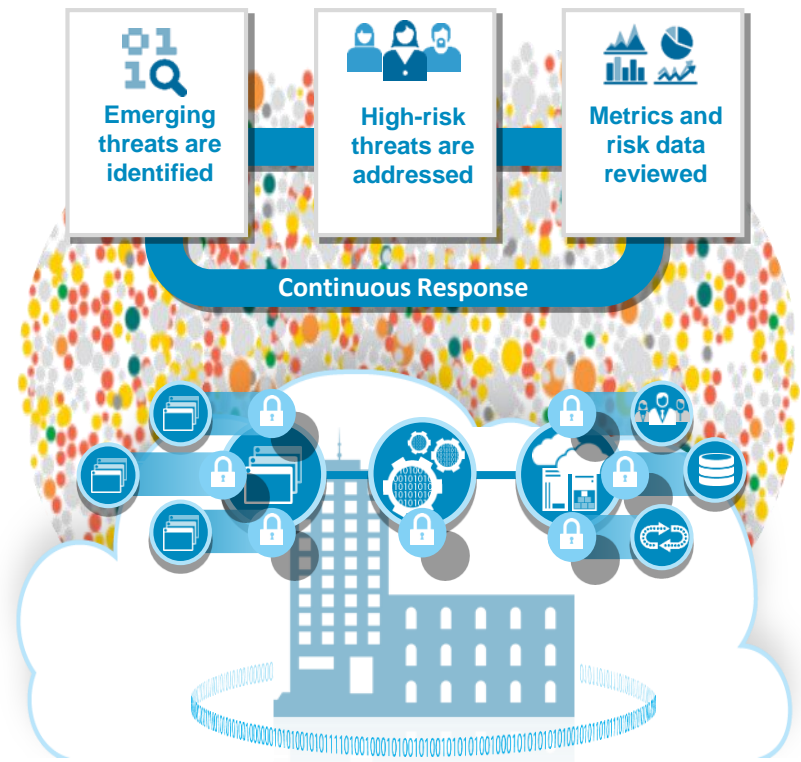
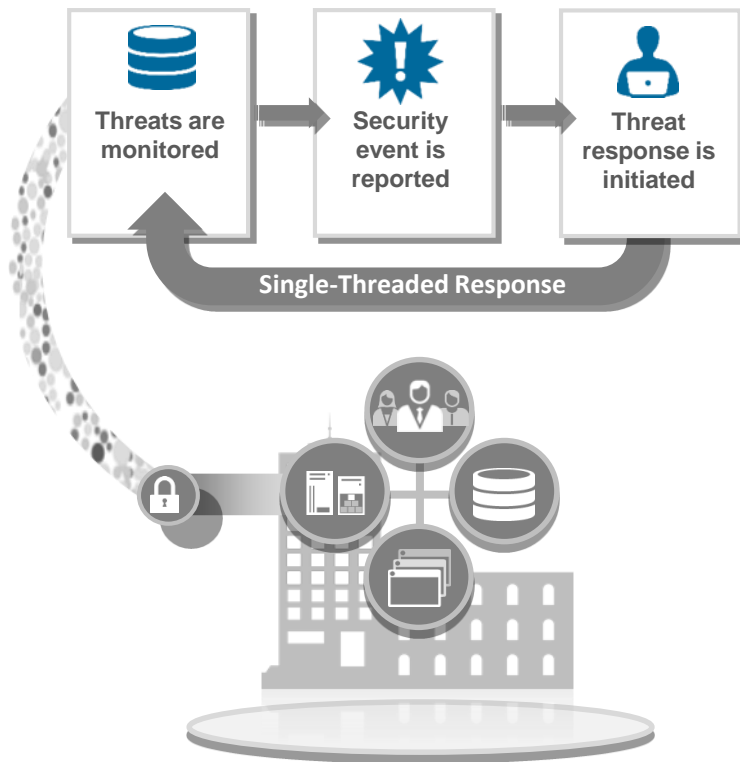
Traditional Managed Security Services:

Management and monitoring of security infrastructure to quickly respond to attacks

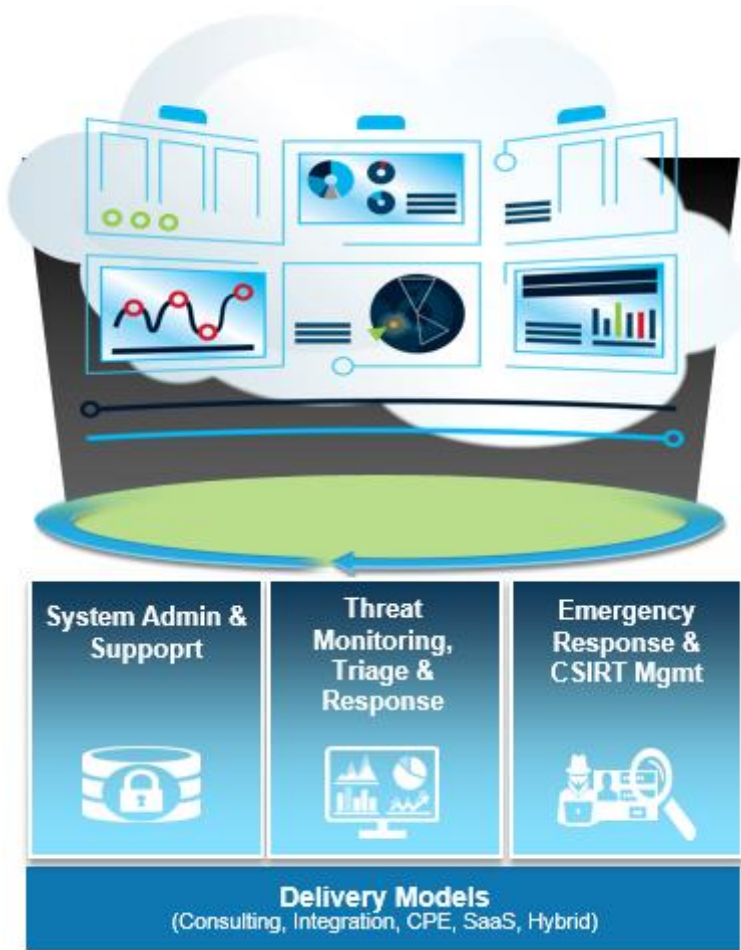


Next-Gen Managed Security Services:

Vast amounts of data yield iterative learning, predictive analytics and a better coordinated defense



Key elements of a next generation managed services architecture



Comprehensive threat insight

- Enable proactive protection

On-demand security services

- The leading consulting and services expertise and capabilities anywhere, anytime

Multiple delivery options

- Cost-effectively optimize the mix of internal/external resources and responsibilities

Unified visibility and control of the security environment

- Make hybrid enterprise IT security manageable

Optimizing the Hybrid IT Approach



- **Single pane of glass view of enterprise security** that encompasses on premise, hosted, outsourced and hybrid delivery options.
- **Integrates Big Data. Intelligence, analytics, reporting and monitoring capabilities** for real-time response and increased protection.
- **Optimizes and simplifies enterprise security operations** with flexible, scalable and cost-effective delivery options.

Providing real business value:

- 90% reduction in emergency response and patching activity
- Average 55% cost reduction vs. doing it in-house
- Handle 99% of events without human intervention
- Protect against new threat remediation 30+ days before market fixes are available
- Manage operations & proactively protect with predictive insights to improve service

A financial services firm teams with IBM to build its first SOC

Optimize Your Security Investments

Identified and blocked

650+

suspicious incidents
in the first 6 months
of SOC operations



Business Challenge

- The bank did not have the security skills and resources to build its first SOC within the aggressive milestones set by their Board
- Wanted global protection for 16,000,000 accounts across 44 countries

IBM Security Solution benefits

- Provides automated, real-time advanced analytics to evaluate 13M+ events per day from 400K+ assets and 28K+ active log sources
- Provides 24x7 SOC management and incident response support at ~\$2M lower cost than in-house management

IBM Security has global reach



IBM Security by the Numbers

133+ monitored countries (MSS)

3300+ service delivery experts

20000+ devices under contract

2700000000+ endpoints protected

15000000000+ events managed per day

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

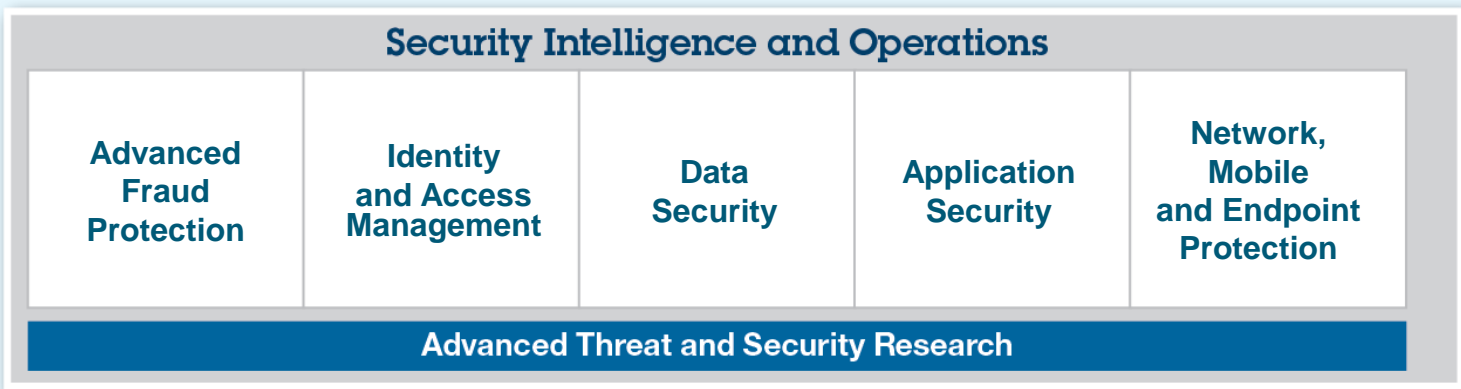


© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

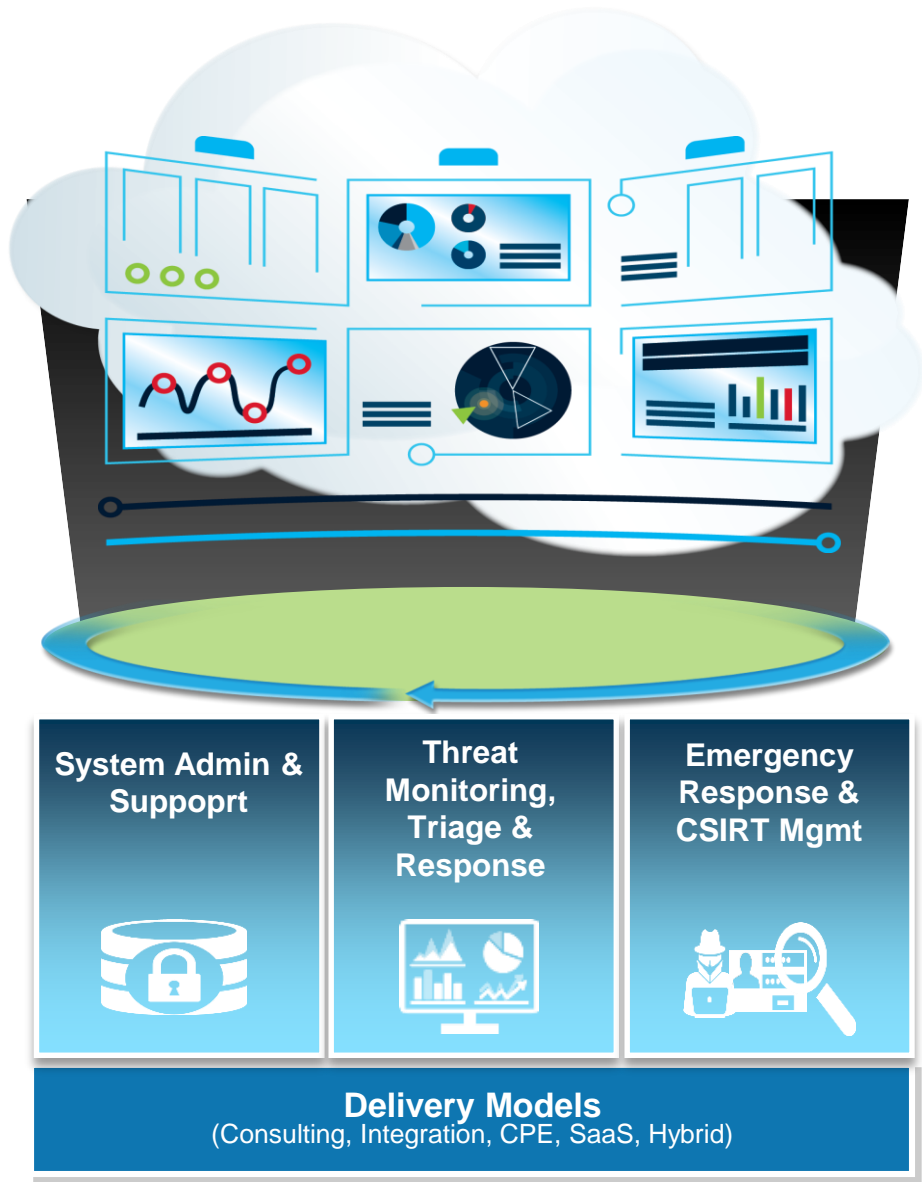
Delivering Next-Gen Managed Security Services



Enabling enhanced, as-you-like-it security services



Next-Gen IBM Managed Security Services



Provide security anywhere, anytime, anyway for hybrid IT environments

IBM Managed Security Services are:

OPEN + SECURE

Technology and data-agnostic, with a platform that's extensible for you to adopt cloud, mobile, and social platforms securely

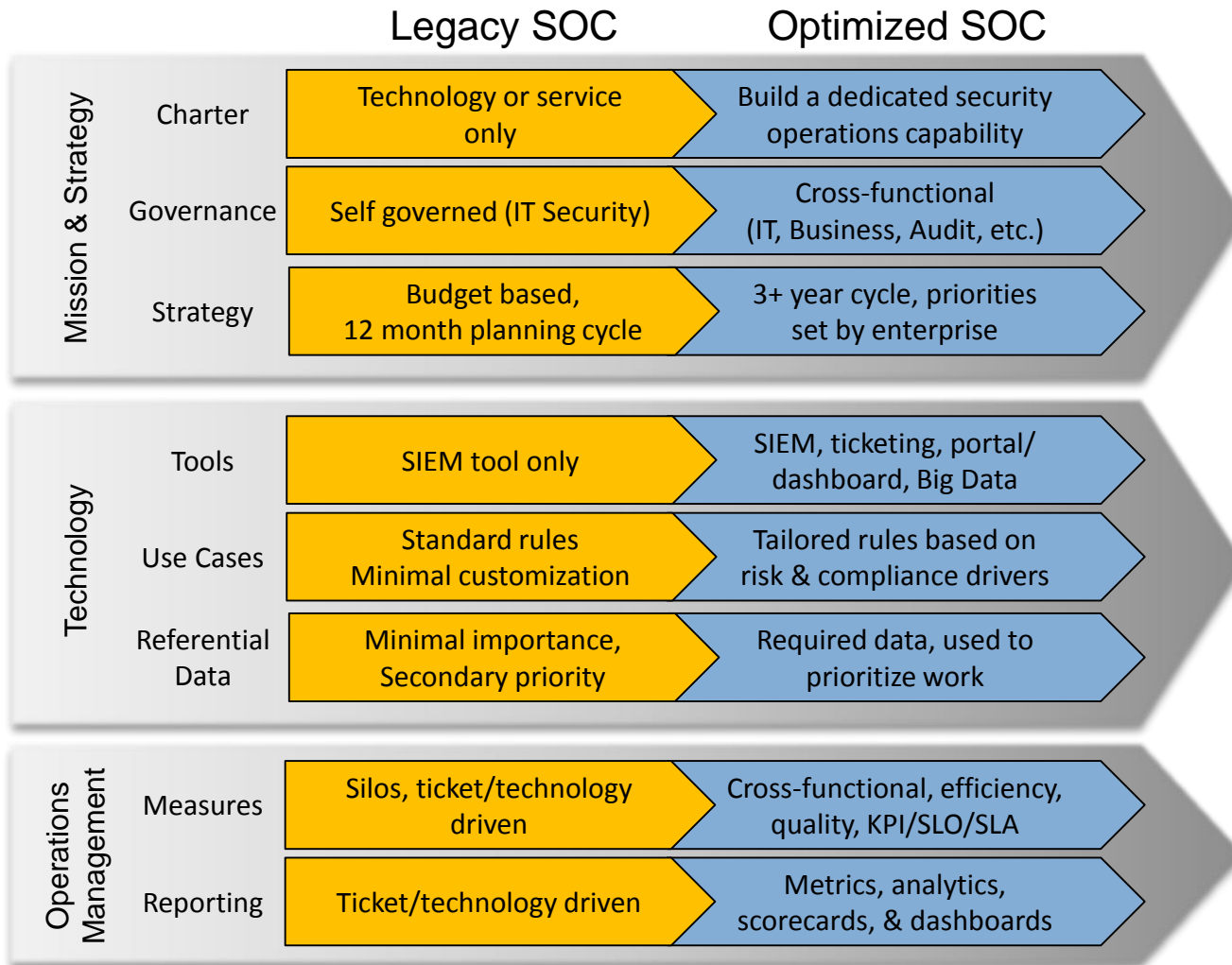
DYNAMIC + INDUSTRIAL STRENGTH

On-demand hybrid security, with the ability to provide security anywhere, anytime, anyway, and a flexible level of management that can provide hardened support

GLOBAL + PERSONAL

Capabilities and footprint enabling IBM visibility at a global level, which can be applied to optimize a client's security posture at a personal level

Security leaders must shift their requirements for enterprise security & risk management and adopt a more transformational approach to SOC design and administration



Detect & react to threats.

*Proactive.
Visible.
Anticipate threats.
Mitigate risks.*

