Notice on Names and Logos Used in This Presentation

NON-IBM PRODUCT AND SERVICE NAMES, LOGOS, AND BRANDS ARE PROPERTY OF THEIR RESPECTIVE OWNERS.

ALL COMPANY, PRODUCT AND SERVICE NAMES USED IN THIS WEBSITE ARE FOR IDENTIFICATION PURPOSES ONLY.

USE OF THESE NAMES, LOGOS, AND BRANDS DOES NOT IMPLY ENDORSEMENT.

IBM Security

Cyber Protection Redefined:

The Security Immune System

Prof. Yaron Wolfsthal
Head of IBM Security Center of Excellence, Israel

wolfstal@il.ibm.com

June 27, 2018

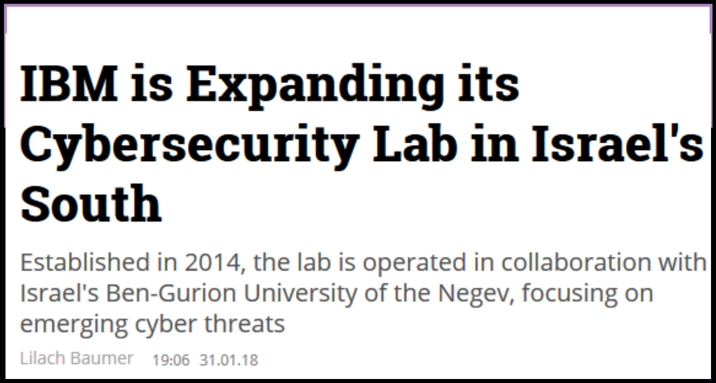
Scope of This Presentation

- Introduction
- Shipping Industry & Cyber Security
- Human Immune System
- Security Immune System
- Select Assets and Applications
- How IBM Can Help

IBM Cybersecurity Center of Excellence

- Joint initiative of IBM and Ben-Gurion University
- Missioned to accelerate security innovation to market
- Close work with clients, e.g., National CERT of Israel

Date	Milestone
2014	Established
2015	First Deliveries
2016 2017	Broad Impact across IBM Security Division
1/18	Expanding to B/S Cyber Park



IBM is Expanding its Cybersecurity Lab in Israel's South

Established in 2014, the lab is operated in collaboration with Israel's Ben-Gurion University of the Negev, focusing on emerging cyber threats

Lilach Baumer 19:06 31.01.18

IBM Cybersecurity Center of Excellence : Activities

- Innovation group for IBM Security Division
  - Tight collaboration with Security product teams
  - Research in new directions

Quad9

Watson for Cyber Security

- Client facing
  - Government agencies
  - Enterprise clients

- Academic collaboration with BGU & more

Ben-Gurion University
of the Negev

Partnerships & Collaborative Innovations

In 2007, MIT scientist Peter Gloor published a seminal paper on the concept of

"Collaborative Innovation Network"

"a cyberteam of self-motivated people with a collective vision... achieving a common goal by sharing ideas, information, and work."

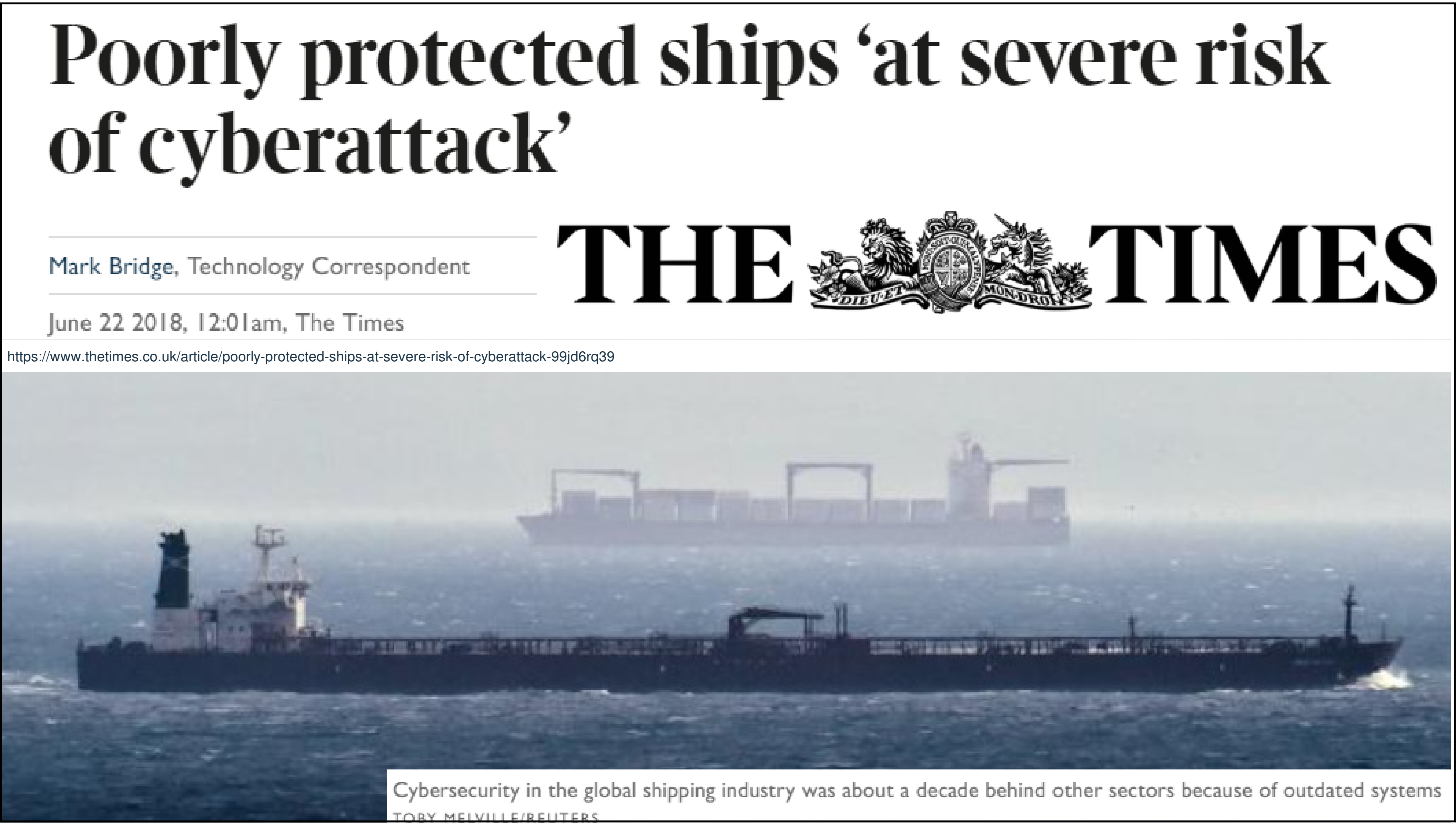
Shipping is the Life Blood of the Global Economy

- 90% of world trade
- 50,000 merchant ships trading internationally
- Fleet registered in 150 nations, manned by over a 1,000,000 seafarers of virtually every nationality
- Technically sophisticated (larger hi-tech vessels can cost over US $200M to build)
- Merchant ships generate an annual income of over half a trillion USD in freight rates

Source:

International Chamber of Shipping
Shaping the future of shipping

- **Ships are a Critical Infrastructure at a Global Scale**



Poorly protected ships 'at severe risk of cyberattack'

THE TIMES

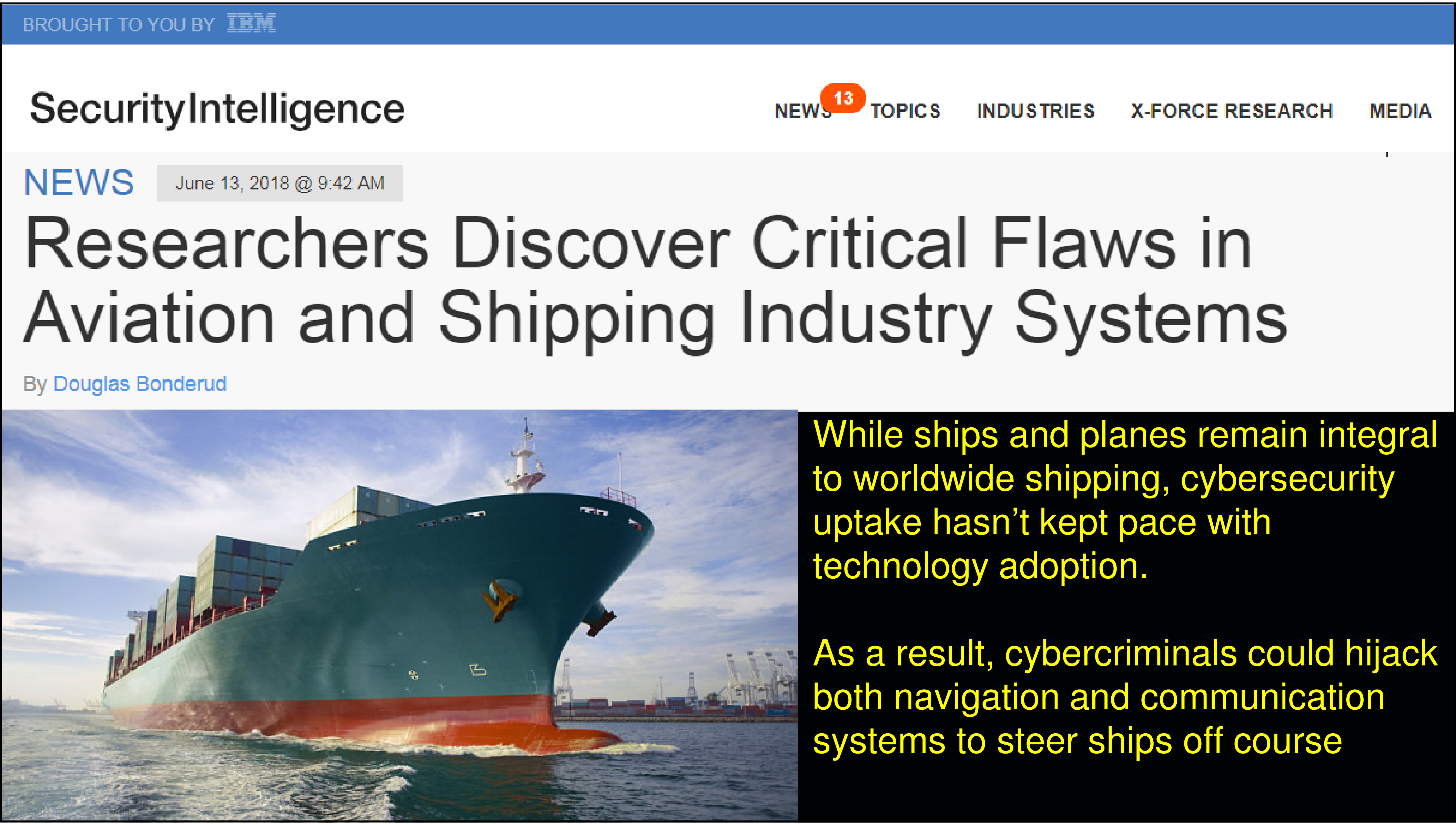
Mark Bridge, Technology Correspondent

June 22 2018, 12:01am, The Times

https://www.thetimes.co.uk/article/poorly-protected-ships-at-severe-risk-of-cyberattack-99jd6rq39

Cybersecurity in the global shipping industry was about a decade behind other sectors because of outdated systems

TOBY MELVILLE/REUTERS



BROUGHT TO YOU BY IBM

SecurityIntelligence

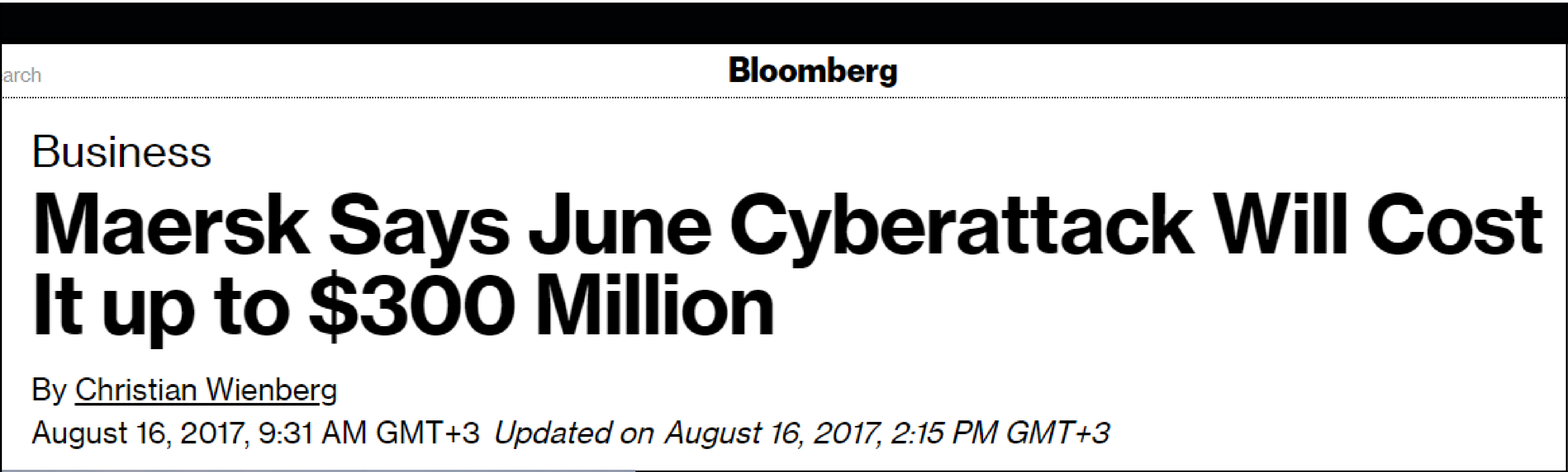
NEWS June 13, 2018 @ 9:42 AM

Researchers Discover Critical Flaws in Aviation and Shipping Industry Systems

By Douglas Bonderud

While ships and planes remain integral to worldwide shipping, cybersecurity uptake hasn’t kept pace with technology adoption.

As a result, cybercriminals could hijack both navigation and communication systems to steer ships off course



arch

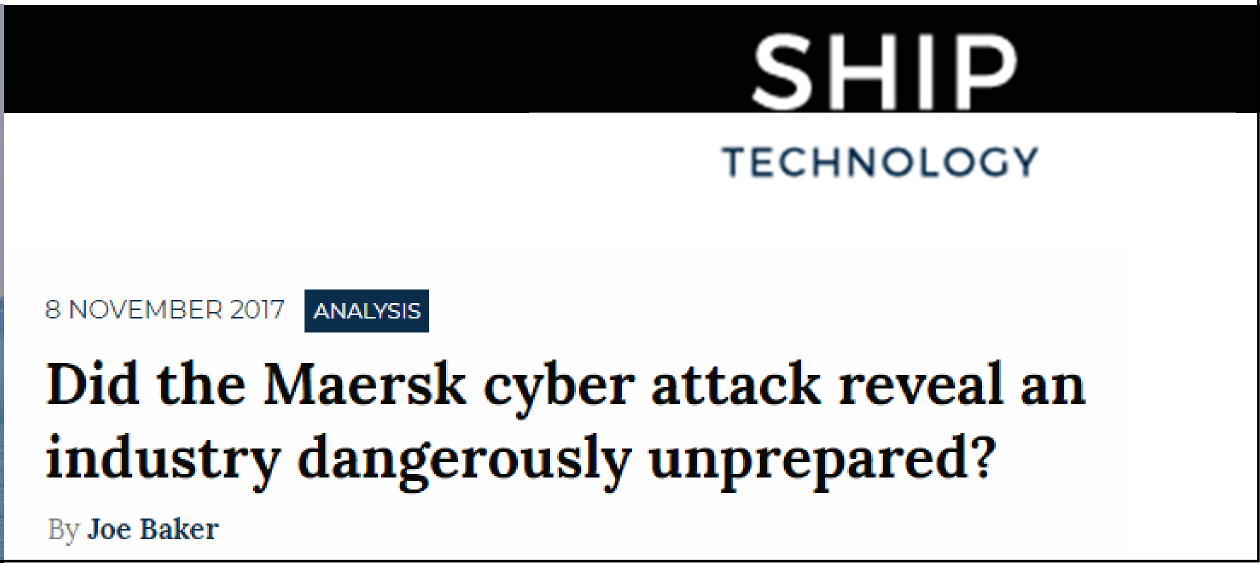
Bloomberg

Business

Maersk Says June Cyberattack Will Cost It up to $300 Million

By Christian Wienberg

August 16, 2017, 9:31 AM GMT+3 *Updated on August 16, 2017, 2:15 PM GMT+3*



SHIP
TECHNOLOGY

8 NOVEMBER 2017 ANALYSIS

Did the Maersk cyber attack reveal an industry dangerously unprepared?

By Joe Baker

Stakes are High. What is the Industry Doing About It?

85 security tools from **45** vendors

1.5 **MILLION** unfilled security positions by 2020

HOPING IT’S NOT ME

BUILDING MORE BARRICADES

SKIPPING THE BASICS

CHECKING AUDIT BOXES

BLOCKING THE CLOUD

ADDING MORE TOOLS

BETTING ON BYOS

IGNORING PRIVILEGES

Adding More Tools – with Little Impact

Data access control

Incident response

Data monitoring

Sandboxing

Log, flow, data analysis

Access management

IP reputation

Content security

Application security management

Firewalls

Antivirus

Criminal detection

Privileged identity management

Incident and threat management

Entitlements and roles

Endpoint patching
and management

Malware protection

Fraud protection

Vulnerability management

Workload
protection

Identity management

Transaction protection

Anomaly detection

Application scanning

Threat sharing

Indicators of compromise

Virtual patching

Cloud access
security broker

Network visibility

Device management

CHANGE

The Human Immune System

- The human immune system is finely tuned—and highly adaptive— to fight off all kinds of attacks on the human body. Cells, tissues and organs work together to fight “foreign” invaders, and can instantly recognize an invader and take action to either block its entry or destroy it.

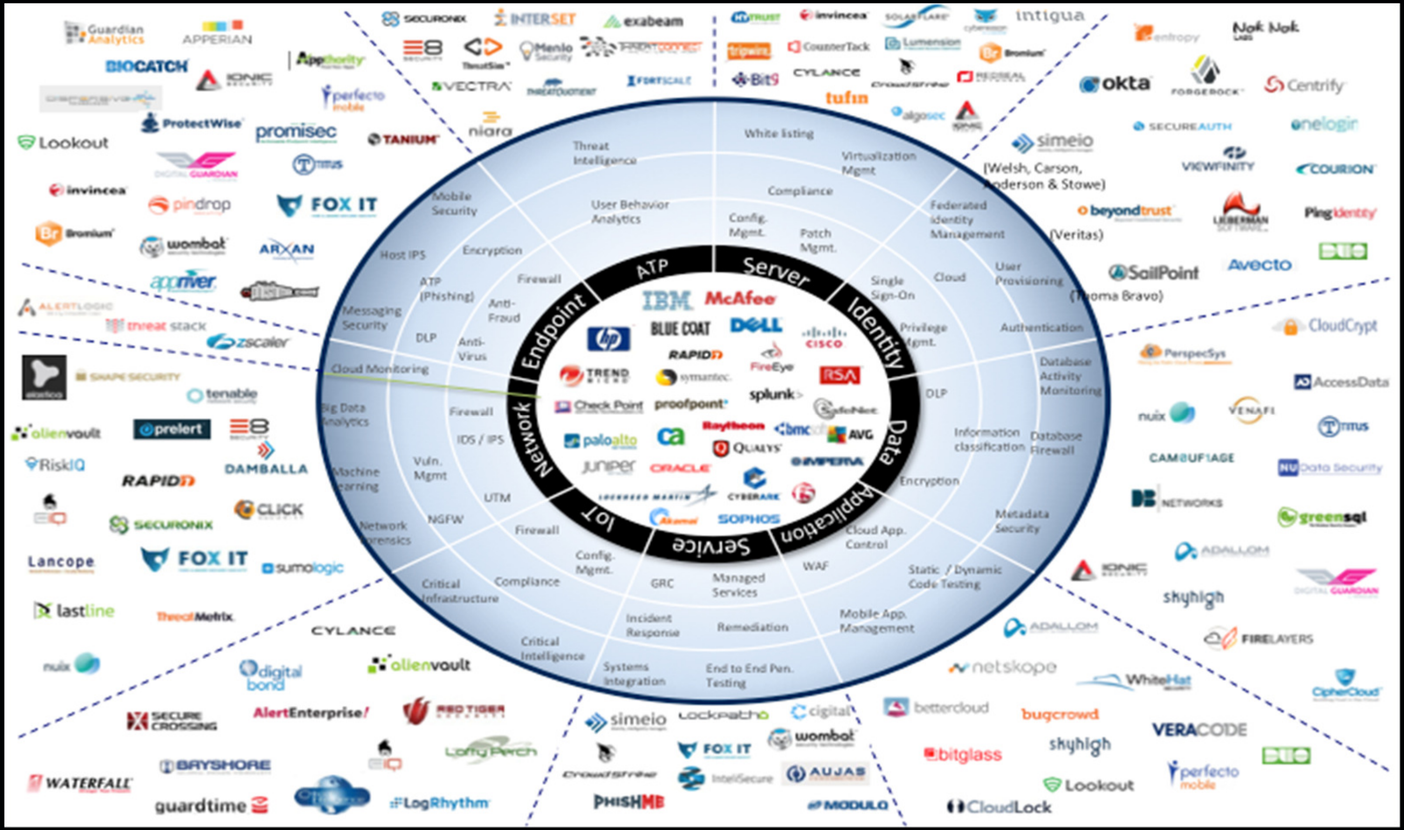
The Human Immune System: Lines of Defense

- Generic/Native Defenses (~1 day)
  - Skin and membranes
  - White blood cells
  - Inflammatory response

- Specific/Adaptive Defenses (~1-7 weeks)
- Second line of defenses
  - Lymphocytes (B & T Cells)
  - Antibodies

In Contrast: How Society Tends to View Cyber Security

Common trend to view cyber security as a diverse collection of technologies, algorithms, products — each designed with a specific target in mind.



- Imagine What Would Happen if our Bodies Worked Like This!

Securing the Enterprise – IBM Philosophy

The industry should take a holistic view and strive to have an

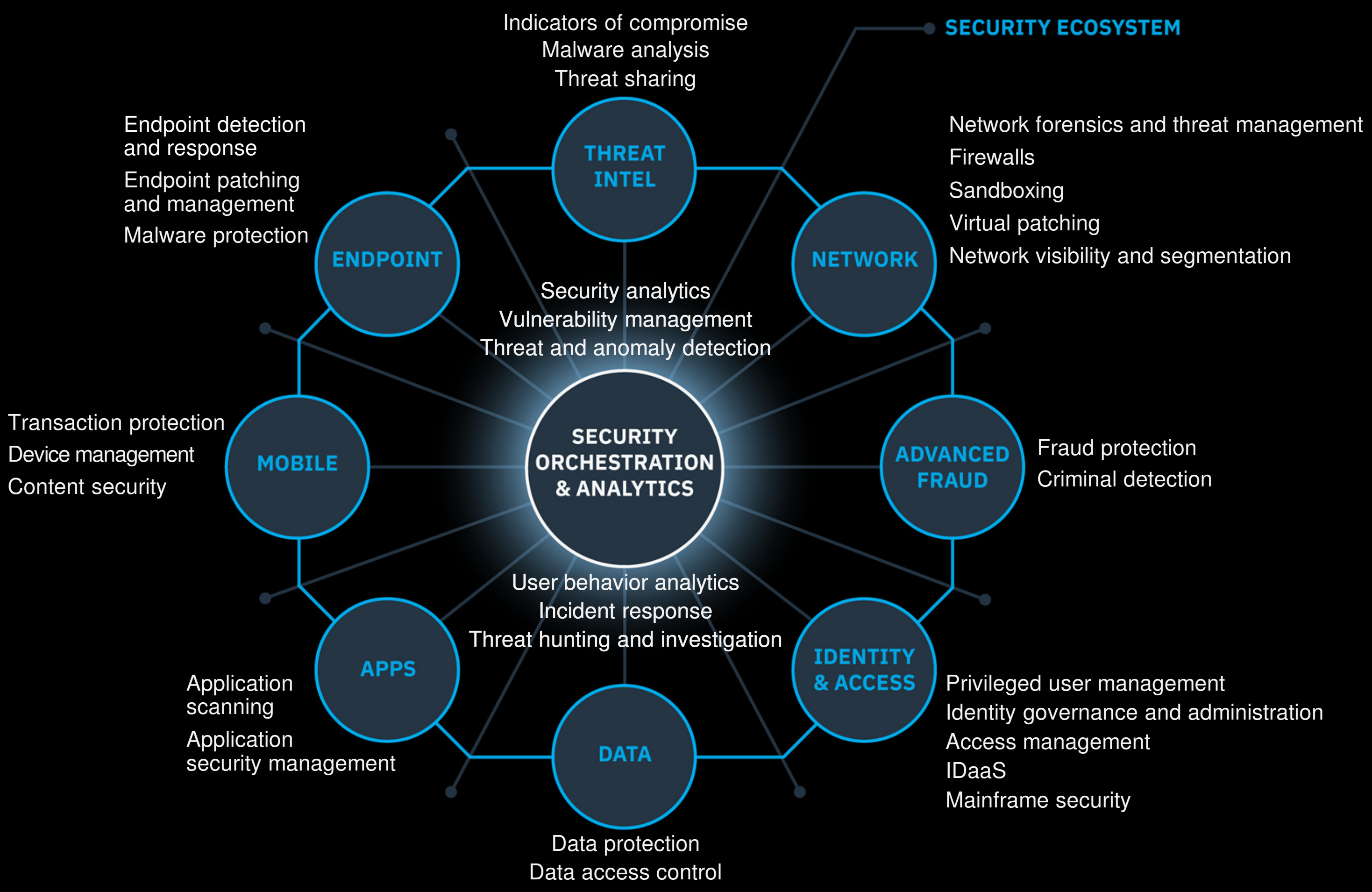
integrated and intelligent security immune system

to counter emerging security threats

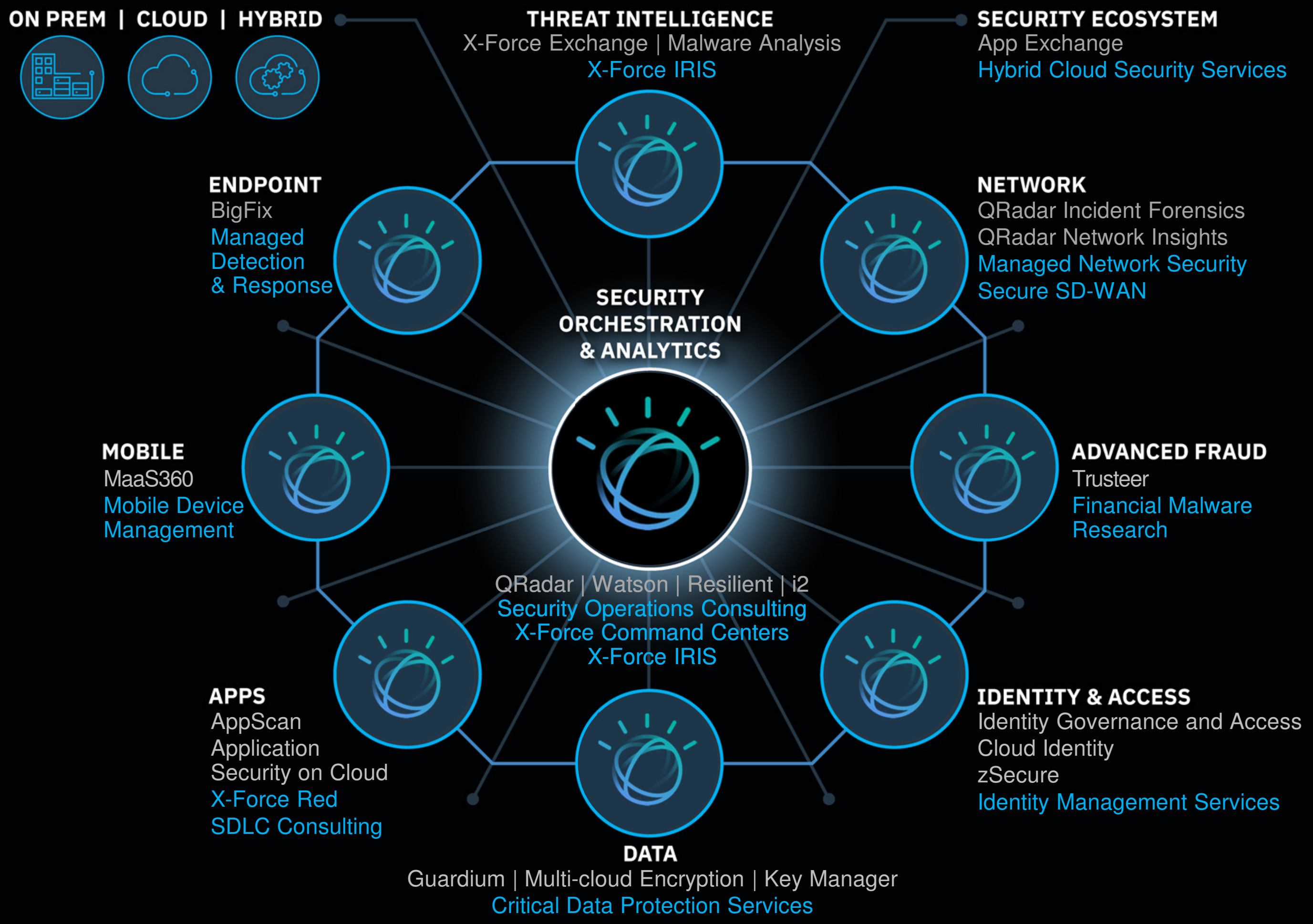
much in analogy to the human immune system.

Our research roadmap based on this vision

An Integrated and Intelligent Security Immune System



Changing the Game with AI



ON PREM | CLOUD | HYBRID

THREAT INTELLIGENCE
X-Force Exchange | Malware Analysis
X-Force IRIS

SECURITY ECOSYSTEM
App Exchange
Hybrid Cloud Security Services

ENDPOINT
BigFix
Managed Detection & Response

NETWORK
QRadar Incident Forensics
QRadar Network Insights
Managed Network Security
Secure SD-WAN

SECURITY ORCHESTRATION & ANALYTICS
QRadar | Watson | Resilient | i2
Security Operations Consulting
X-Force Command Centers
X-Force IRIS

MOBILE
MaaS360
Mobile Device Management

ADVANCED FRAUD
Trusteer
Financial Malware Research

APPS
AppScan
Application Security on Cloud
X-Force Red
SDLC Consulting

IDENTITY & ACCESS
Identity Governance and Access
Cloud Identity
zSecure
Identity Management Services

DATA
Guardium | Multi-cloud Encryption | Key Manager
Critical Data Protection Services

Products
Services

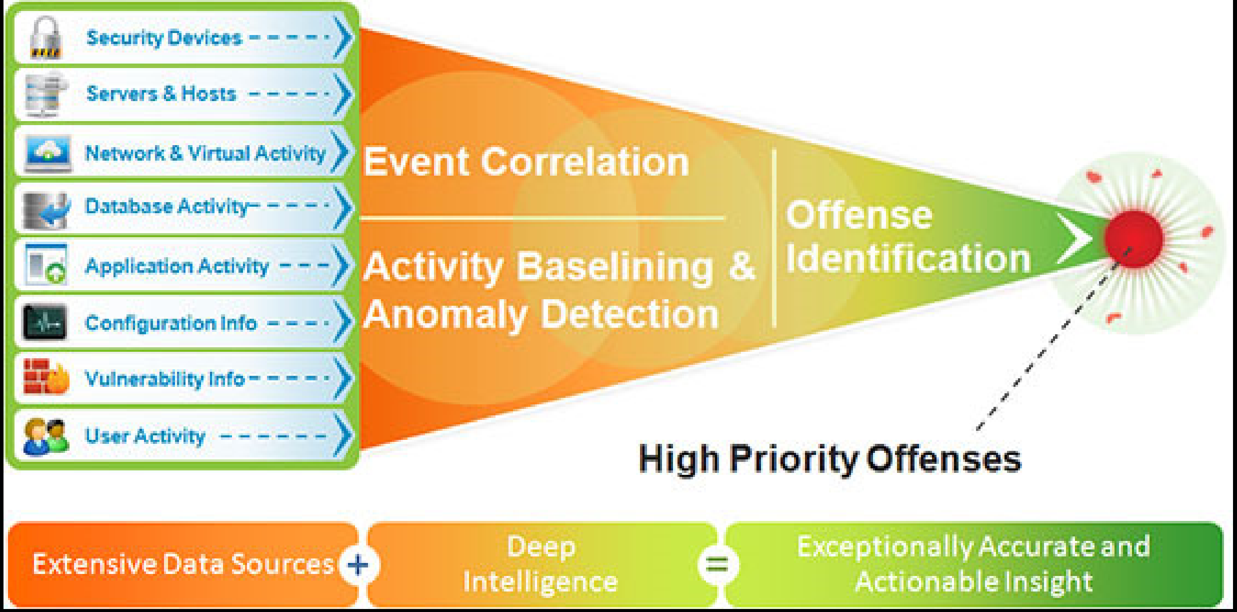
IBM Security

SECURITY IMMUNE SYSTEM: SAMPLE ASSETS & APPLICATIONS

The Centerpiece: Security Information & Event Management (SIEM)

- Collects security-related information and events from a variety of sources.
- Events forwarded to a centralized management console, which performs analysis and flags anomalies.

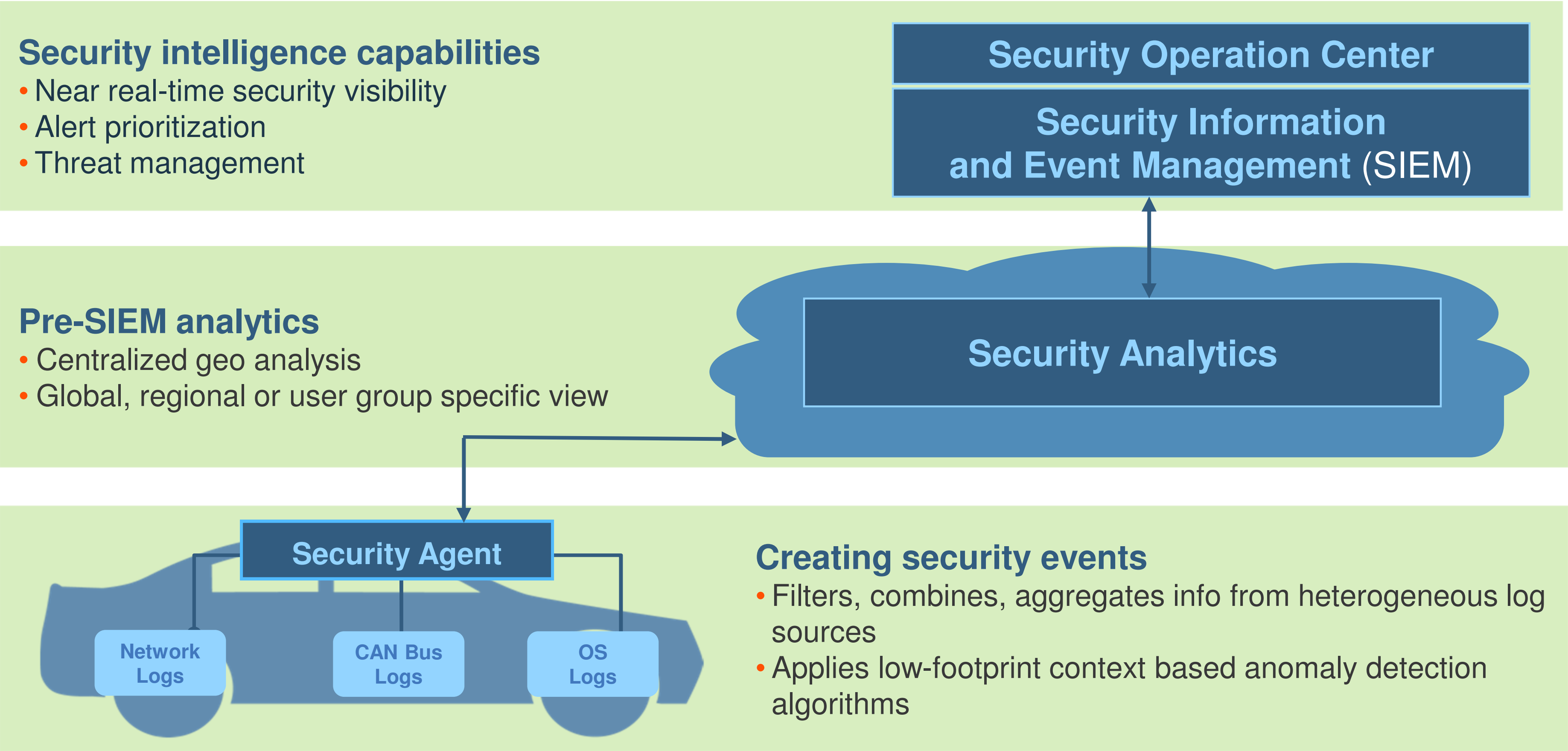
- Key capabilities
  - Data aggregation
  - Correlation
  - Alerting
  - Dashboards
  - Compliance
  - Retention
  - Forensic analysis
  - 1M ‘s of EPS



According to Gartner, IBM QRadar is a market leader in Security Information and Event Management (SIEM)

IBM Connected Vehicle Security Intelligence Solution

***Edge-based security architecture** can be applied to other industries/Use cases.*



Security intelligence capabilities

- Near real-time security visibility
- Alert prioritization
- Threat management

Security Operation Center

Security Information and Event Management (SIEM)

Pre-SIEM analytics

- Centralized geo analysis
- Global, regional or user group specific view

Security Analytics

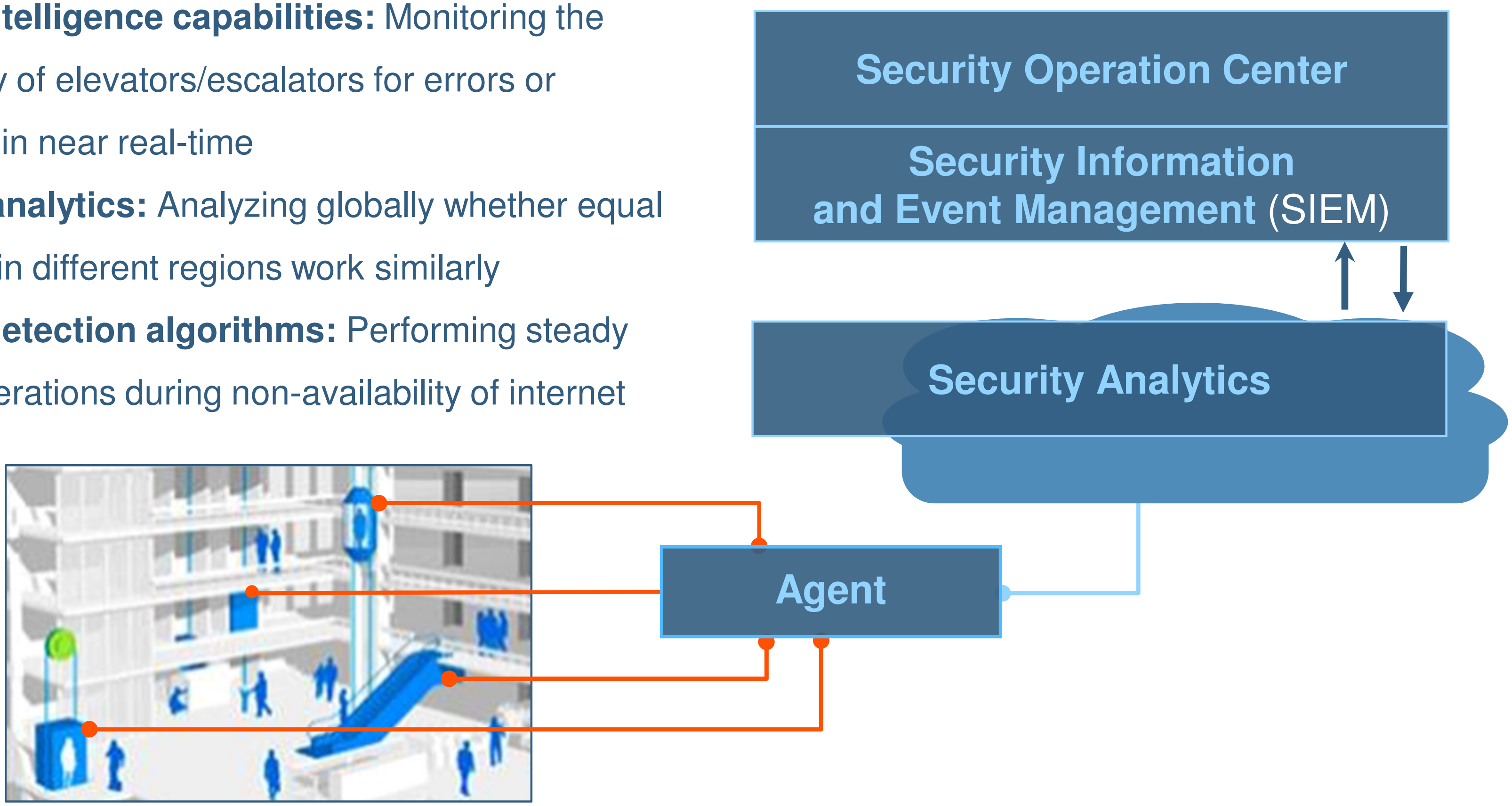
Security Agent

Creating security events

- Filters, combines, aggregates info from heterogeneous log sources
- Applies low-footprint context based anomaly detection algorithms

IBM Security Intelligence Solution for Smart Buildings

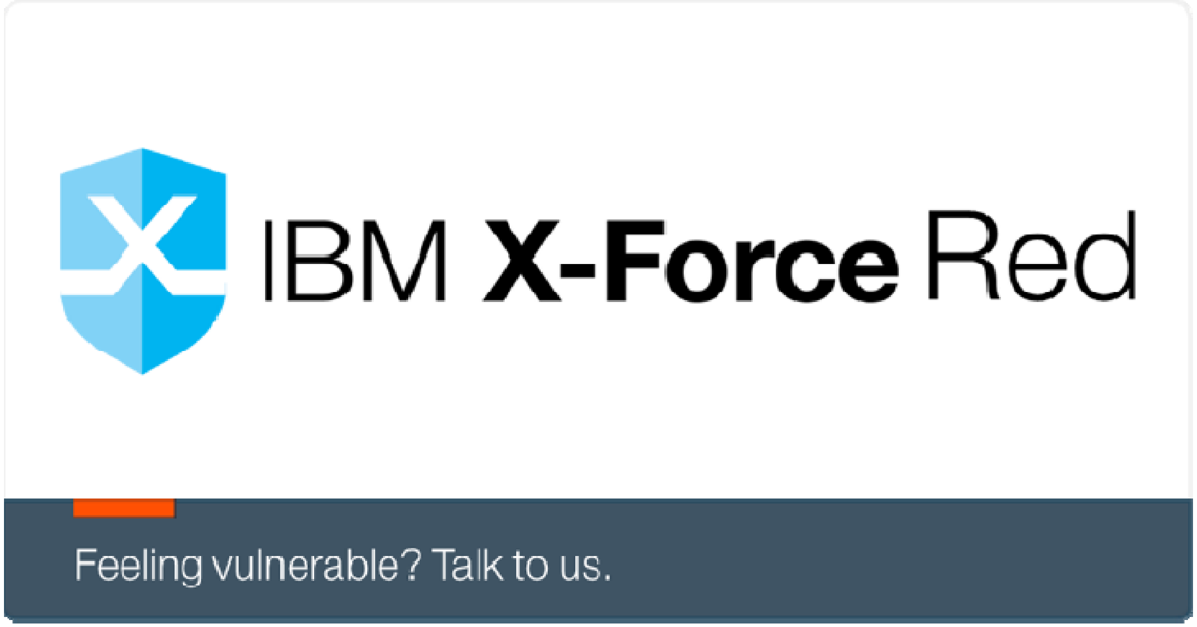
- **Security intelligence capabilities:** Monitoring the functionality of elevators/escalators for errors or disruptions in near real-time
- **Pre-SIEM analytics:** Analyzing globally whether equal equipment in different regions work similarly
- **Anomaly detection algorithms:** Performing steady security operations during non-availability of internet


Security Operation Center
Security Information and Event Management (SIEM)
Security Analytics
Agent

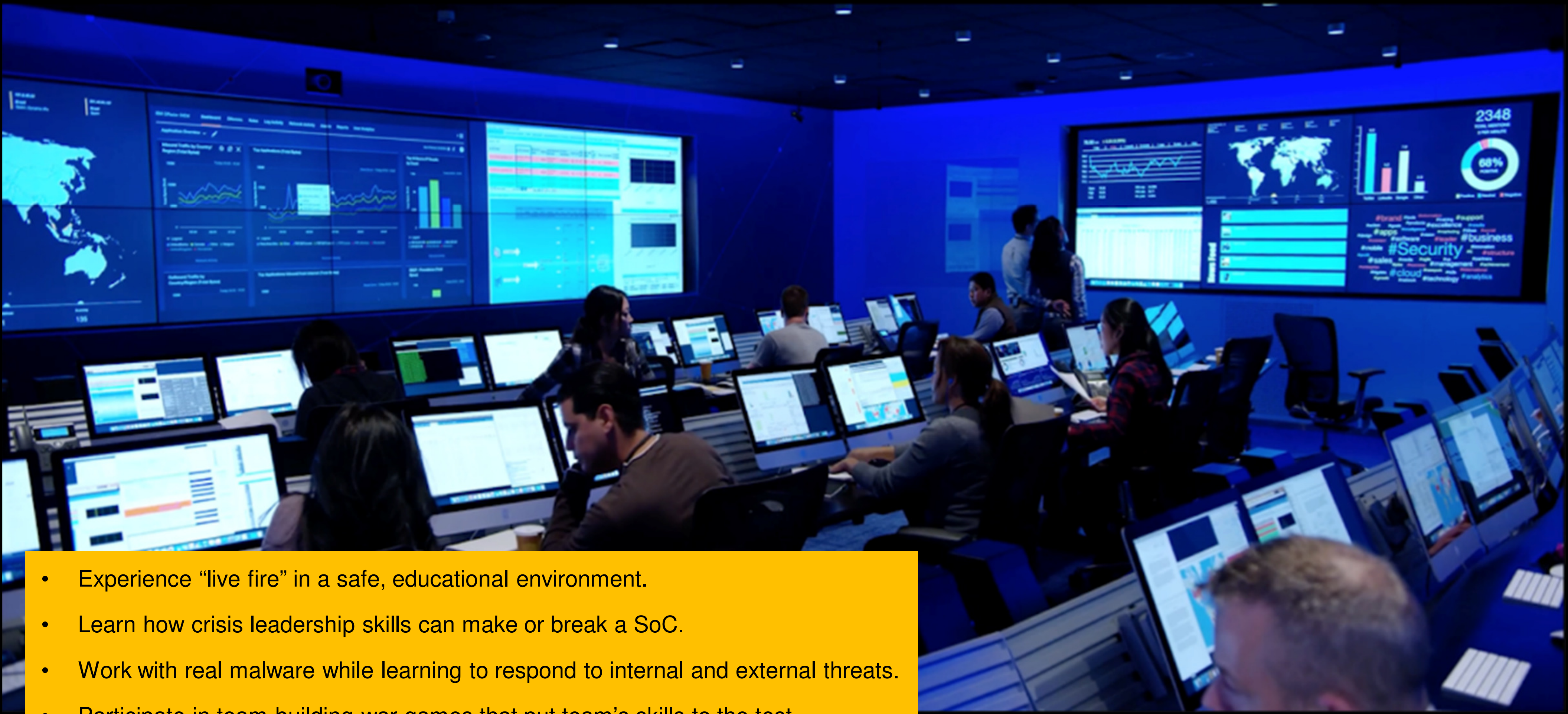
IBM Security

SECURITY IMMUNE SYSTEM: ORGANIZATIONAL ASSESSMENTS

INTERNET OF THINGS (IOT)
PARADISE FOR HACKERS !

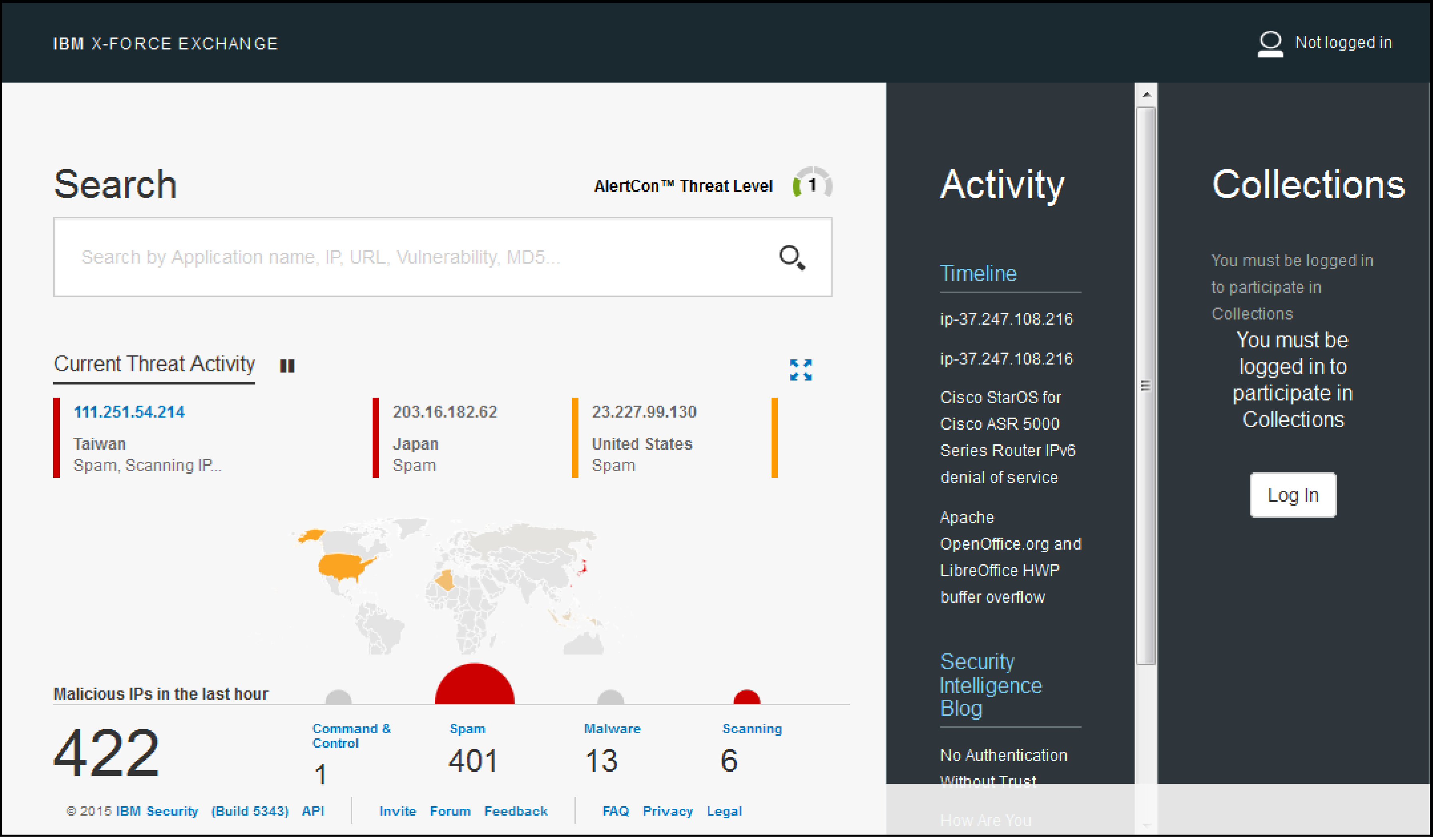


The IBM Security Cyber Range



- Experience “live fire” in a safe, educational environment.
- Learn how crisis leadership skills can make or break a SoC.
- Work with real malware while learning to respond to internal and external threats.
- Participate in team-building war games that put team’s skills to the test.

Threat Sharing Using X-Force Exchange



IBM X-FORCE EXCHANGE

Not logged in

Search

AlertCon™ Threat Level 1

Search by Application name, IP, URL, Vulnerability, MD5...

Current Threat Activity

111.251.54.214
Taiwan
Spam, Scanning IP...

203.16.182.62
Japan
Spam

23.227.99.130
United States
Spam

Malicious IPs in the last hour

422

Command & Control	Spam	Malware	Scanning
1	401	13	6

© 2015 IBM Security (Build 5343) API | Invite Forum Feedback | FAQ Privacy Legal

Activity

Timeline

ip-37.247.108.216

ip-37.247.108.216

Cisco StarOS for Cisco ASR 5000 Series Router IPv6 denial of service

Apache OpenOffice.org and LibreOffice HWP buffer overflow

Security Intelligence Blog

No Authentication Without Trust

How Are You

Collections

You must be logged in to participate in Collections

You must be logged in to participate in Collections

Log In

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

wolfstal@il.ibm.com

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.

IBM