Cyber Threat Intelligence for Defense

Dr. Charles Li, CTO, GBS Cyber Security and Biometrics, IBM

Bruce Cerretani, Federal Lead Solution Architect, IBM
Cyber attackers break through conventional safeguards every day

Source: IBM X-Force Threat Intelligence Index - 2017

average time to identify data breach

201 days

average cost of a U.S. data breach

$7 M

#GOVANALYTICS2017
Who is attacking?

The majority of all attacks in 2014 and 2015 were carried out by **INSIDERS** ... in other words by **people you are likely to trust**.
Traditional security practices are unsustainable

- **85** security tools from **45** vendors
- **1.5 MILLION** unfilled security positions by 2020
- **68 PERCENT** of CEOs are reluctant to share incident information externally
#1 For Project Managers: Cybersecurity is about mission and cost effectiveness

**Current State of Cybersecurity**

*CYBERSECURITY*

We have limited resources and our end users don’t fully appreciate the threats we face.

**Desired State of Cybersecurity**

- Reducing Cost
- Increasing Quality
- Measurable Results

**Improved Cyber Defense**
#2 For Practitioners: One Pane of Glass providing actionable information

Current State of Cybersecurity

Desired State of Cybersecurity

MONITOR FATIGUE

The last thing we need is yet another system to worry about.
Integrated security, analytics and exploration

- Structured
- Analytical
- Repeatable

Security Intelligence Platform

- Real-time Processing
  - Real-time data correlation
  - Anomaly detection
  - Event and flow normalization
  - Security context & enrichment
  - Distributed architecture

- Security Operations
  - Pre-defined rules and reports
  - Offense scoring & prioritization
  - Activity and event graphing
    - Compliance reporting
    - Workflow management

Big Data Platform

- Big Data Processing
  - Long-term, multi-PB storage
  - Unstructured and structured
    - Distributed Hadoop infrastructure
  - Preservation of raw data
  - Enterprise Integration

- Analytics and Forensics
  - Advanced visuals and interaction
  - Predictive & decision modeling
  - Ad hoc queries
    - Interactive visualizations
    - Collaborative sharing tools
    - Pluggable, intuitive UI

Integrated IBM Solution

- Flexible
- Exploratory
- Ad-Hoc
There are **known knowns**; there are things we know we know.

We also know there are **known unknowns**; that is to say we know there are some things we do not know.

But there are also **unknown unknowns**; there are things we do not know we don’t know.

*Donald Rumsfeld, US Secretary of Defense, Feb 2002*

**Today’s Defense in Depth:** Highly centric around Rules & Signatures based detection with non consistent use of advanced machine learning
Cognitive computing: A new capability for a holistic approach

Most SIEM INDICATORS: do not consider non-traditional cyber sources to enrich their situational awareness and detection capabilities and provide little advise on how to deal with an attack.
Intelligence amplification (IA) (also referred to as cognitive augmentation and machine augmented intelligence) refers to the effective use of information technology in augmenting human intelligence.
Cognitive computing changes the defense in depth landscape in a fundamental way

- Employment of advanced Machine Learning techniques that self learn to **adapting** threat attack vectors and tradecraft

- Utilizing and deriving insight from **non-traditional** cyber sources to **augment** classical Cyber detection and Intelligence analysis

- **Intuitive** and **human** like Natural Language interfaces that CISO’s and SOC analyst can derive **Intelligence**

- Ability to ingest and analyze **massive** amounts of real-time and historical

- Providing real-time recommendation and courses of action to **remediate and minimize** cyber attacks
Addressing the cyber challenge with advanced machine learning, analytics and cognitive computing

Watson for Cyber Security offers Deep Learning, Cognitive Cyber Intelligence

Cyber Entity Resolution
Attacker Attribution-Correlation Intelligence

Advanced Cyber Analytics (ACA)

Cyber Forensic Analysis and Remediation

Cognitive

Knowledge Graphs

Analytics

Machine Learning
Advanced Low Observable Detection Appliance

DNS Data
Netflow Data

X-Force
Customer Black & White List
Proxy Logs

CCD Botnet Communication Detector

IBM

Real-time Monitoring
End-Point Management
Target Server

Big Data Analytics
Predictive Models

Network Traffic
Cyber analysts are overwhelmed with the amount of data – that’s beyond human capabilities

**Cognitive Technology** can now:

- Process this data and correlate cyber SIEM/Sensor data with cyber text
- Respond to threats with greater confidence at speed and scale
- And out think and outpace cyber threats

### Manual threat analysis

- Incident Triage
- Investigation and Impact Assessment
- Remediation

### Days to Weeks

---

### IBM Cognitive Technology assisted threat analysis

- Incident Triage
- Investigation and Impact Assessment
- Remediation

### Minutes

---

As a result …
THANK YOU

QUESTIONS?