nic

Future Edition

Watson for Cyber Security

Fighting cyber threats with A.I. and cognitive computing

Victor Grane

Security Solutions Engineer
IBM Security

victor.grane@se.ibm.com

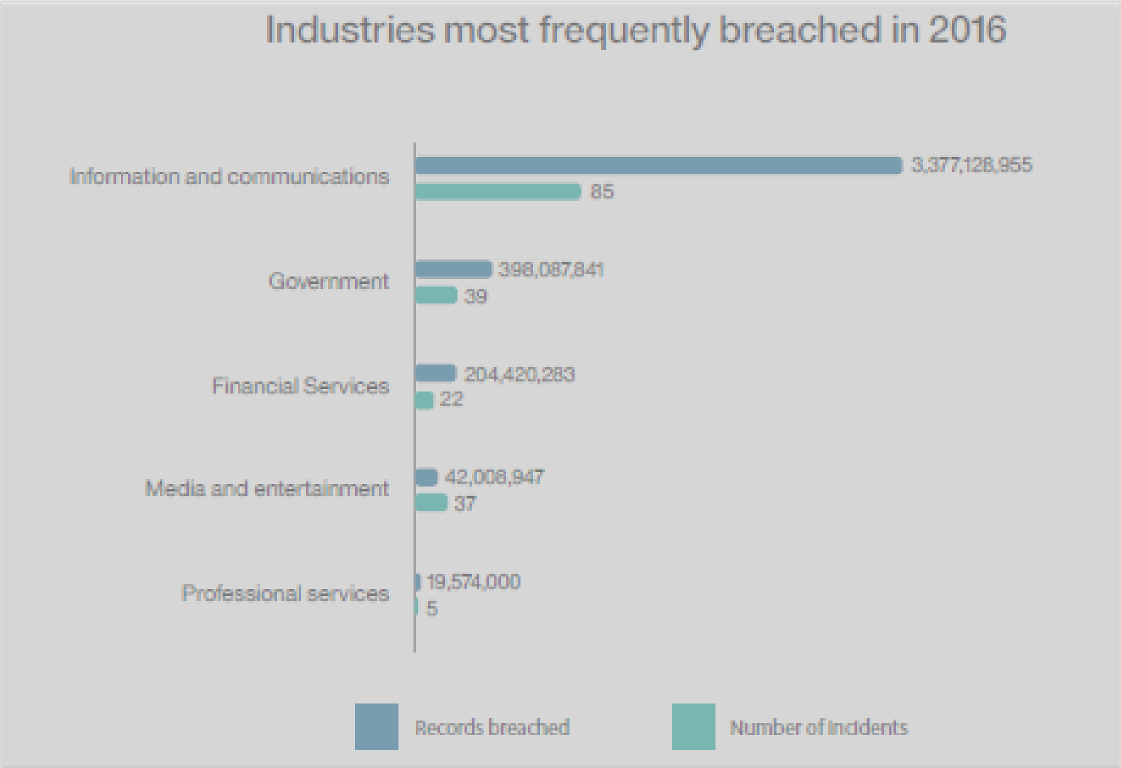
Agenda

- Some observations on today’s cyber security trends
- The evolution of the Security Operations Center
- Machine learning and Cognitive technology in cyber security
- Orchestrating an effective incident response
- Demo of cognitive technology in action

Some observations on today’s cyber security trends

What we have seen

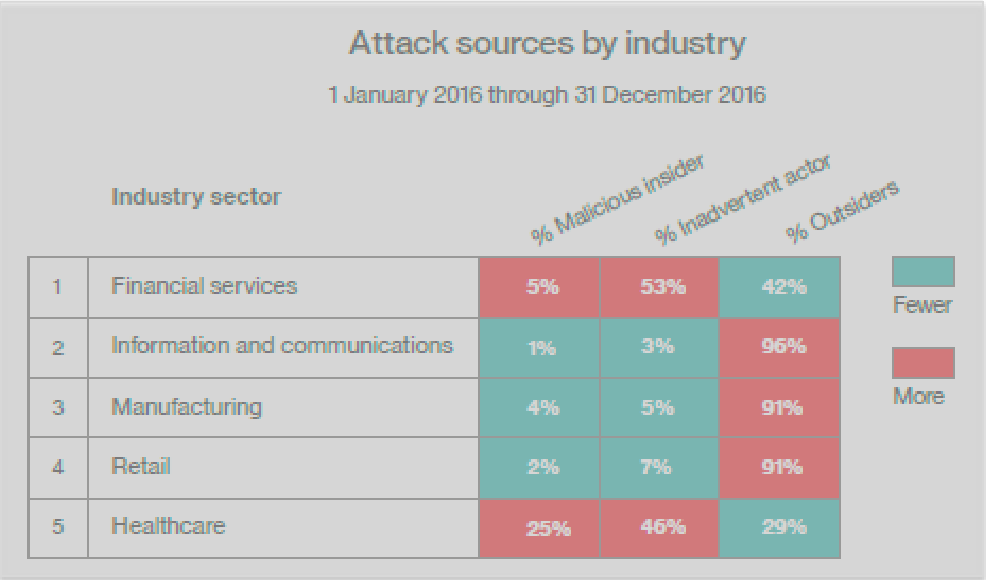
- **Focus industries**
- **Attack patterns**
- **Examples**



IBM X-Force Threat Intelligence Report 2016

Where are the “bad guys”

- **Insider threats: 60-70% of security incidents**
- **Inadvertent actors is a major part**
- **Attack vectors through spam and social engineering**



Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

🟩 Fewer

🟥 More

IBM X-Force Threat Intelligence Report 2016

Responding to threats

What organizations need to do

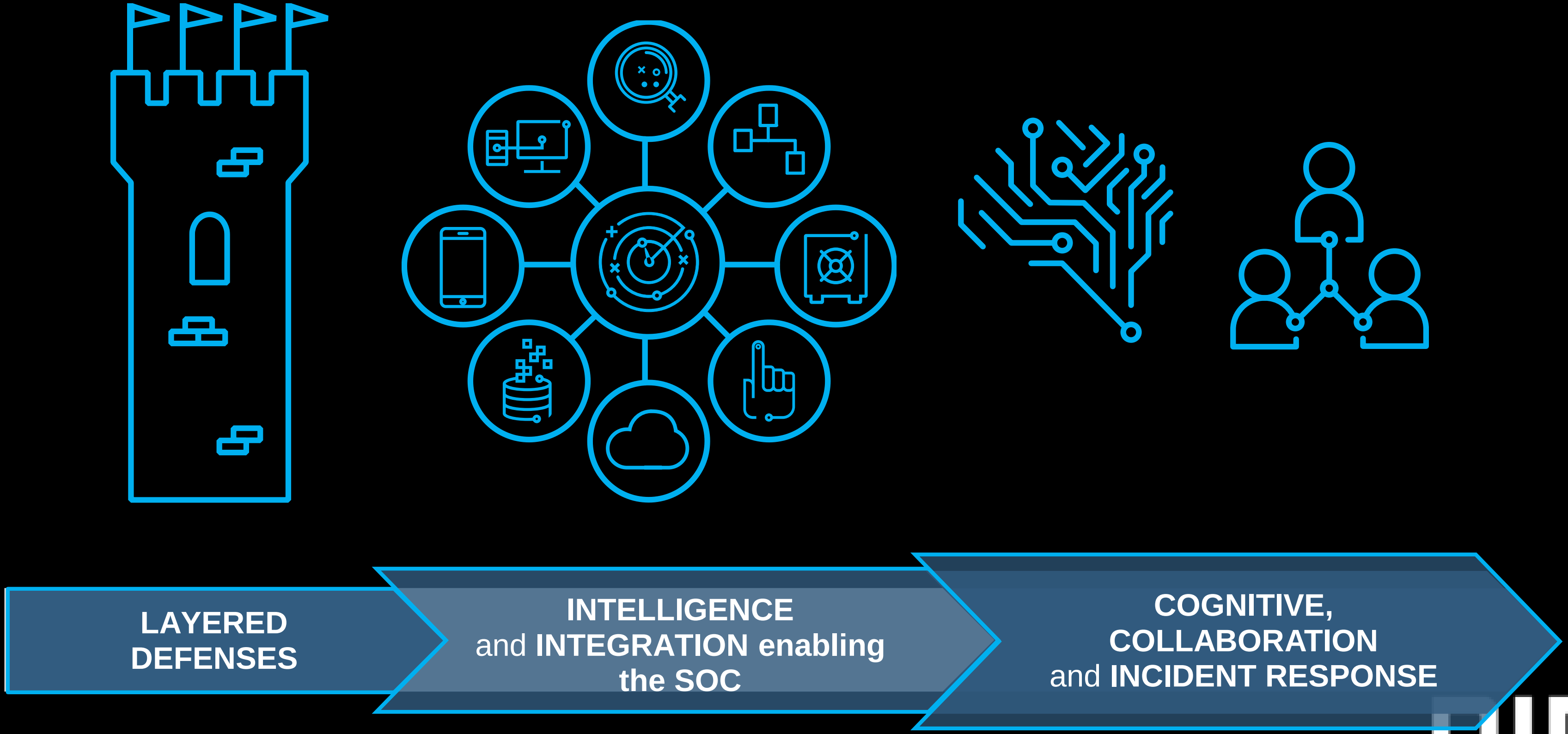
Centralize and streamline **security practices**

Enable and provide **knowledge sharing** within cyber security

Build and operate **SOC and IRP** across your organization

The evolution of the SOC

How is cyber security evolving?

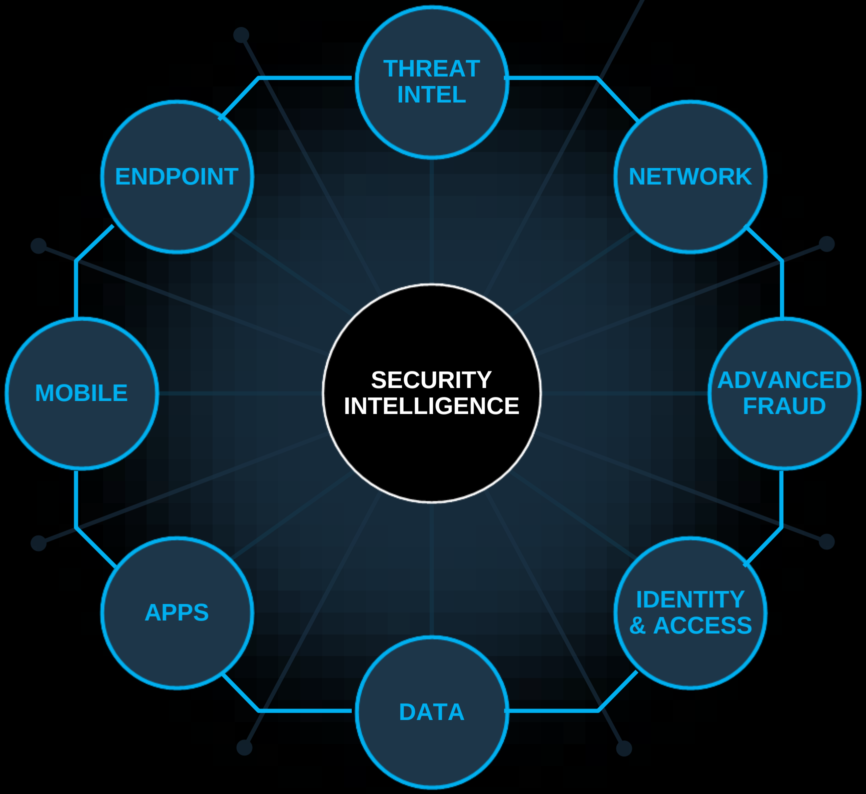


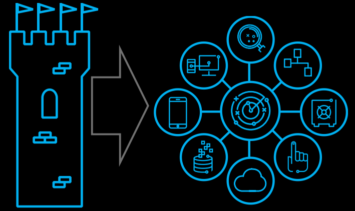
LAYERED DEFENSES

INTELLIGENCE
and INTEGRATION enabling
the SOC

COGNITIVE,
COLLABORATION
and INCIDENT RESPONSE

An integrated and intelligent security “immune” system





Security Intelligence - detecting the needle in the hay stack

EXTENSIVE DATA SOURCES

Security devices

Servers and mainframes

Network and virtual activity

Data activity

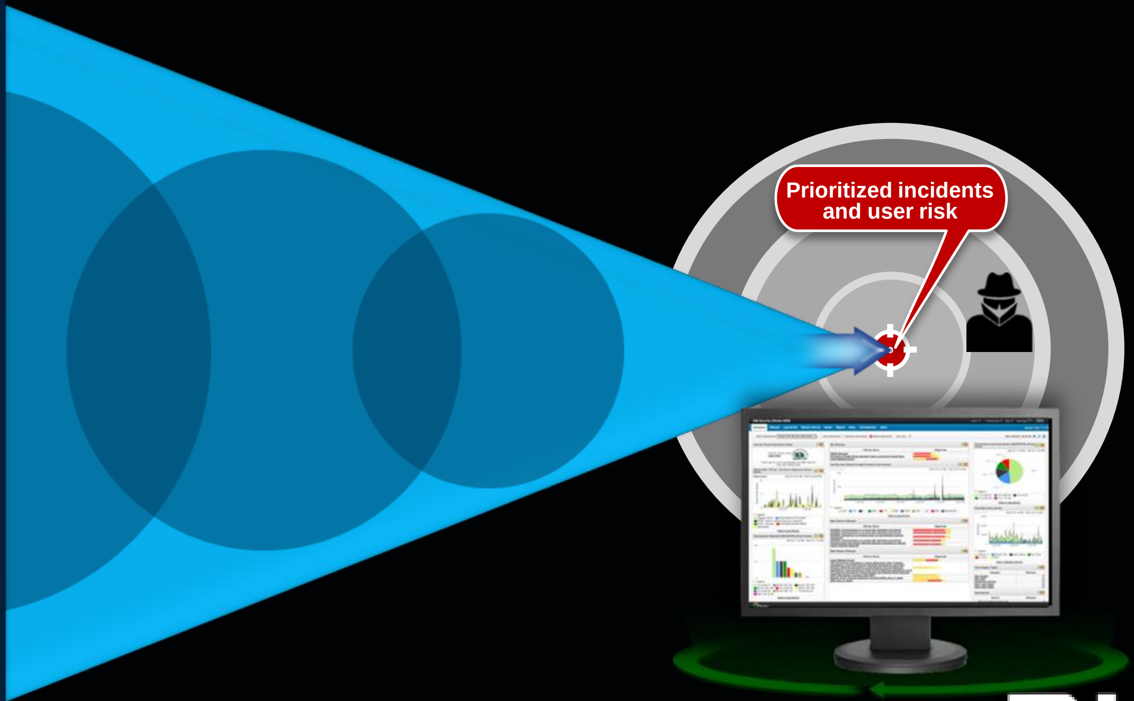
Application activity

Configuration information

Vulnerabilities and threats

Users and identities

Global threat intelligence

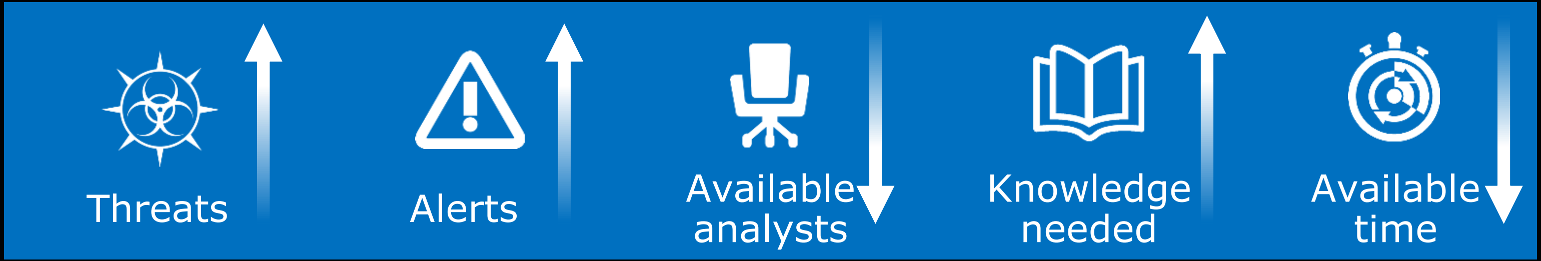


Prioritized incidents and user risk

Moving towards Cognitive security

Challenges for a Security analyst

Quick Insights: Current Security Status



Threats ↑

Alerts ↑

Available analysts ↓

Knowledge needed ↑

Available time ↓

- **Must constantly maintain and monitor defensive measures**
- **Keep current on new threats and vulnerabilities**
- **Greater demand for skilled resources increases costs**
- **Accuracy and responsiveness are essential**

20% of

Security data is structured data and readable by computers.

- **Security events and alerts**
- **Logs and configuration data**
- **Threat and vulnerability feeds**
- **User and network activity**

80% of

Security data is unstructured, created for humans, and inaccessible to traditional systems.

720K

Security blogs per year

180K

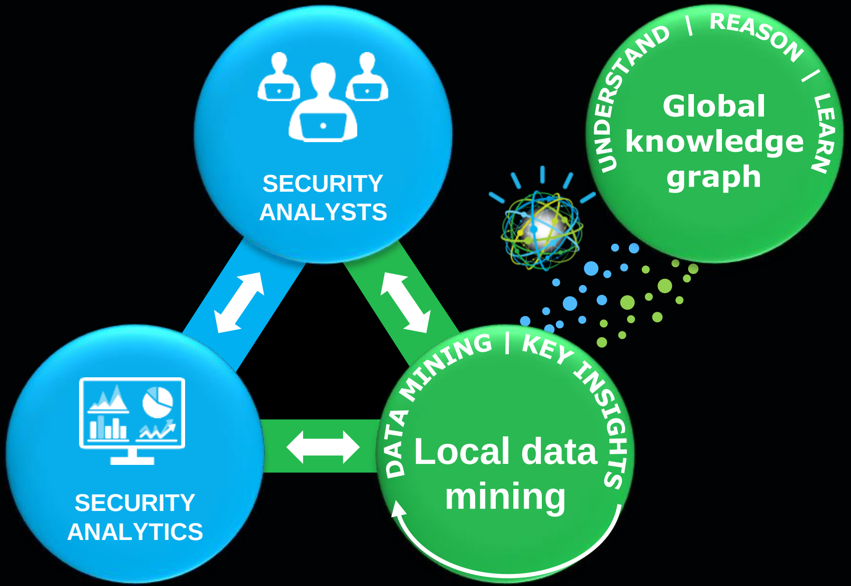
Security related news articles per year

10K

Security research papers per year

- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Tweets

Making Cognitive Security Accessible to the Security Analyst



So what do we do now?

Incident Response

Prevention

Detection

Response

Help to continuously stop attacks and remediate vulnerabilities

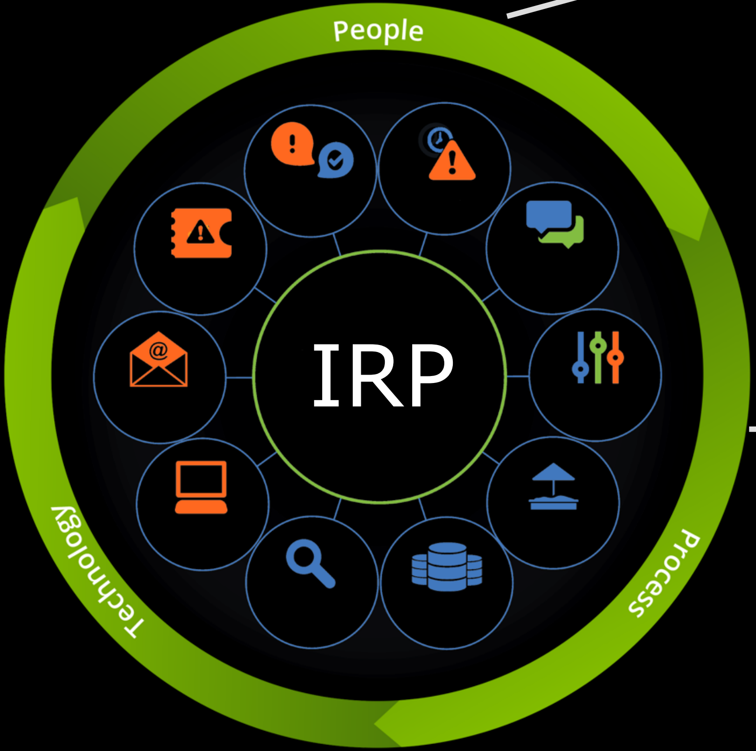
Identify the most important threats with advanced analytics and forensics

Respond to incidents in integrated and organized fashion

Well… we are mastering this…

But we also need this…

Achieving consistancy with Incident Response



- Identifying key resources
- Orchestrating actions

- Defining and automating processes
- Regulations and legal actions

- Collecting and enriching information
- Automate responses processes

Resources

- Security Intelligence: https://securityintelligence.com/category/topics/cognitive/
- Collaboration at X-Force: https://exchange.xforce.ibmcloud.com/
- X-Force Research: https://www.ibm.com/security/resources/xforce/research.html
- X-Force Threat Intelligence Report: https://securityintelligence.com/media/xforce-tir-2016/