COGNITIVE AND AUTONOMIC CYBER DEFENCE

Fred Maymir-Ducharme, Ph.D.,
IBM Federal CTO Office, USA
fredmd@us.ibm.com

Lee Angelelli
IBM Federal CTO Office, USA
langelel@us.ibm.com

Doug Stapleton
IBM Defence, AU
doug.stapleton@hinfosec.com.au

CyberSecurity

CyberSecurity is broader and more complex than traditional Information Security

The size (e.g., data and information) and complexity (inter-relationships between system components and security requirements) continues to grow

CyberSecurity Challenges

Three Levels of Defense

1. ***Protection***
2. ***Detection & Recovery***
3. ***Audits & Logs***

New Cyber Challenges

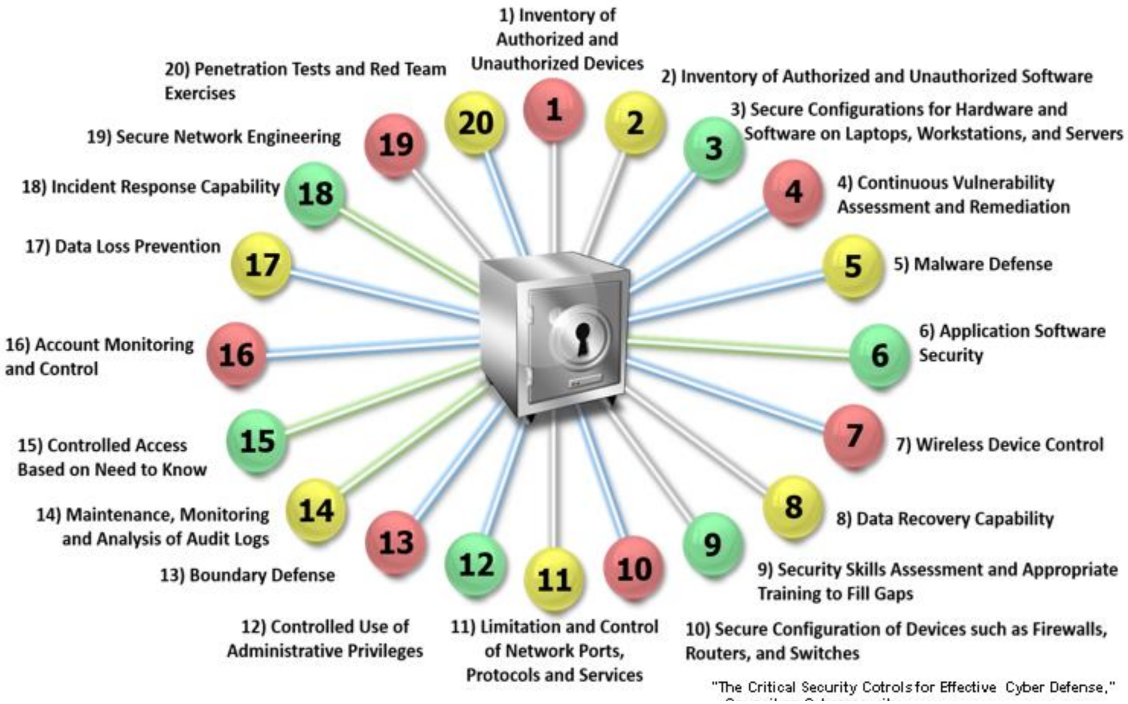
- ***Cloud Platforms***
- ***Mobile Platforms***
- ***Insider Threats***
- ***All is Interconnected***
- ***Cyber Warfare***

Advanced Technology

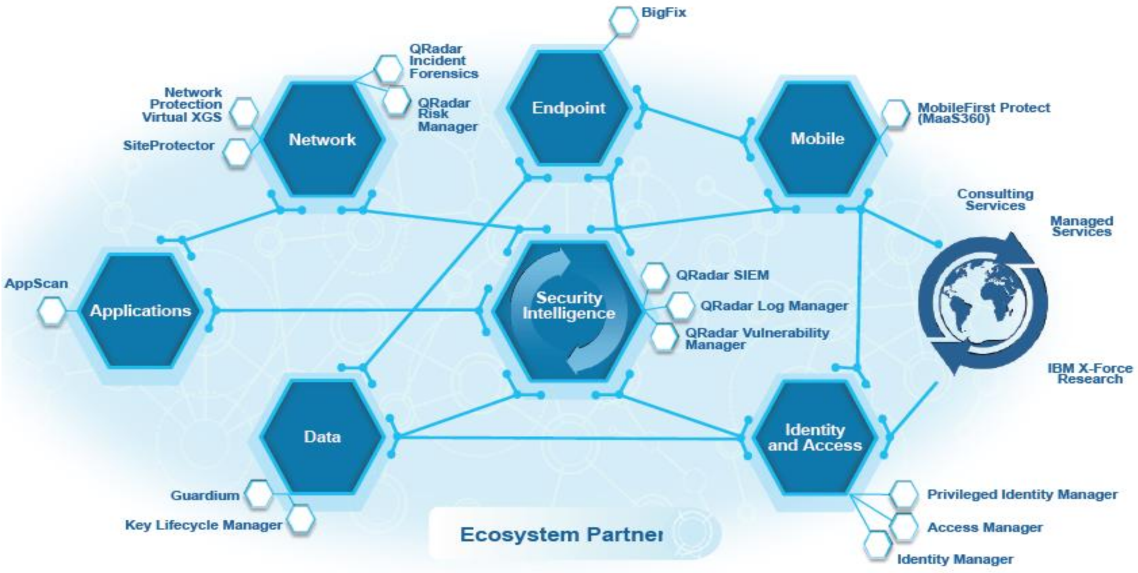
✓ ***Offense***

✓ ***Defense***

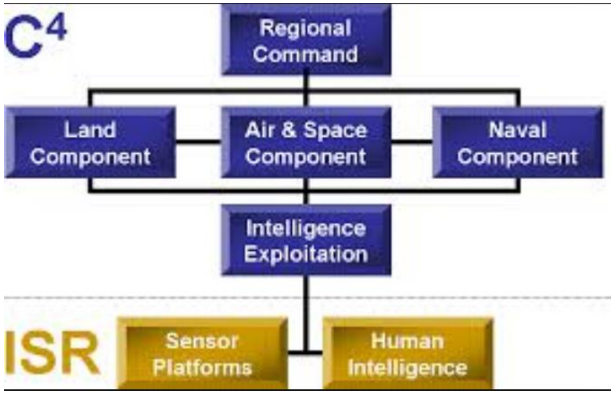
CYBERSECURITY IS CRITICAL SECURITY

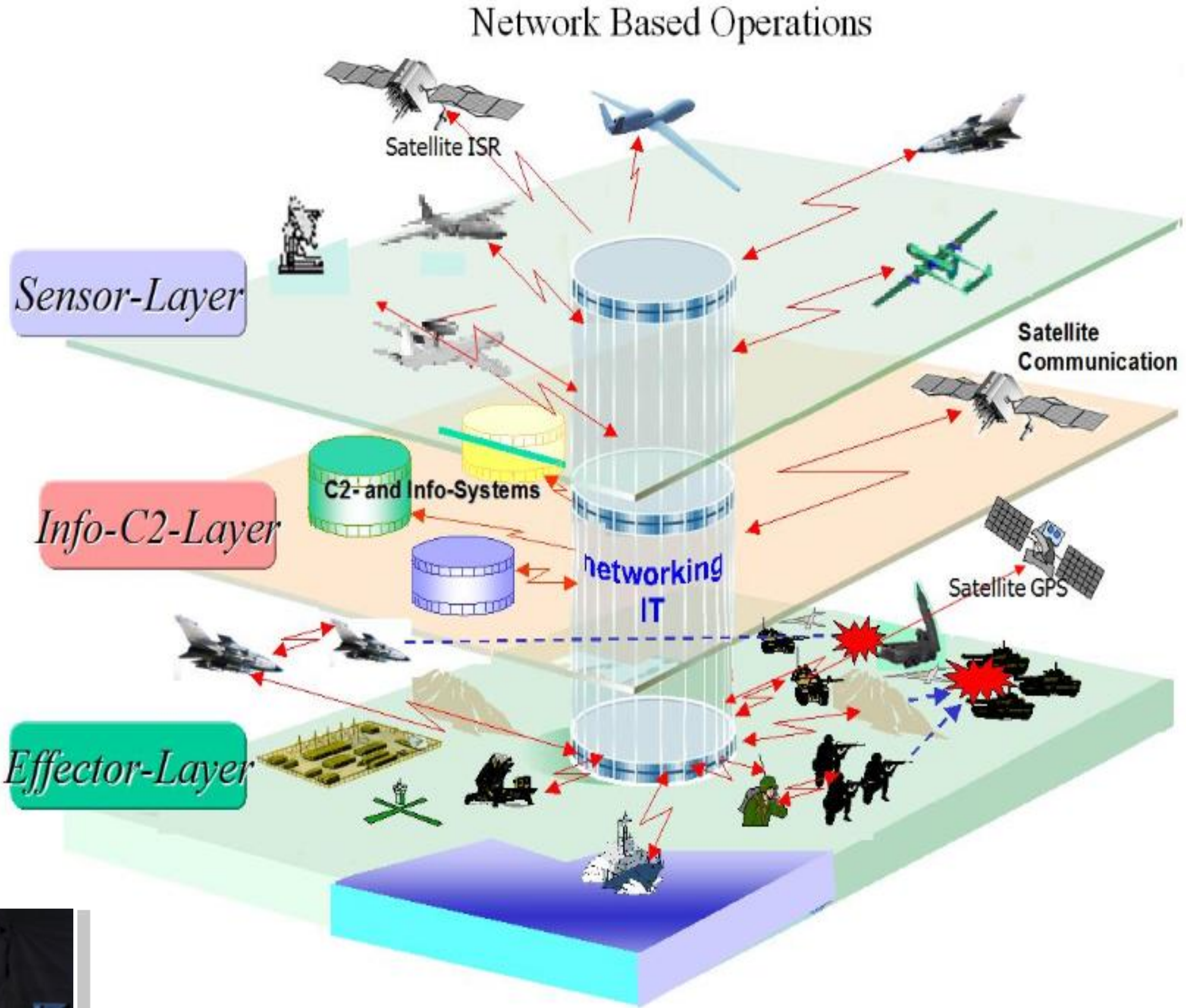

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4) Continuous Vulnerability Assessment and Remediation
5) Malware Defense
6) Application Software Security
7) Wireless Device Control
8) Data Recovery Capability
9) Security Skills Assessment and Appropriate Training to Fill Gaps
10) Secure Configuration of Devices such as Firewalls, Routers, and Switches
11) Limitation and Control of Network Ports, Protocols and Services
12) Controlled Use of Administrative Privileges
13) Boundary Defense
14) Maintenance, Monitoring and Analysis of Audit Logs
15) Controlled Access Based on Need to Know
16) Account Monitoring and Control
17) Data Loss Prevention
18) Incident Response Capability
19) Secure Network Engineering
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

"The Critical Security Cotrols for Effective Cyber Defense,"



NATO Cyber Challenges

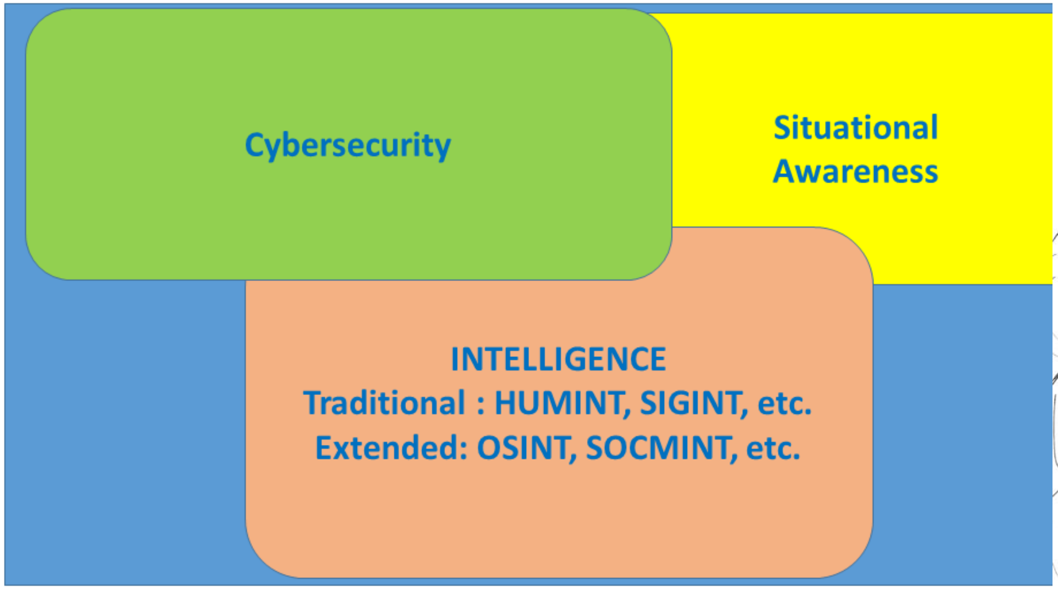




V = f(T,A) :: Vulnerabilities are a function of Threats to Assets

Extending Traditional Scope of Cyber

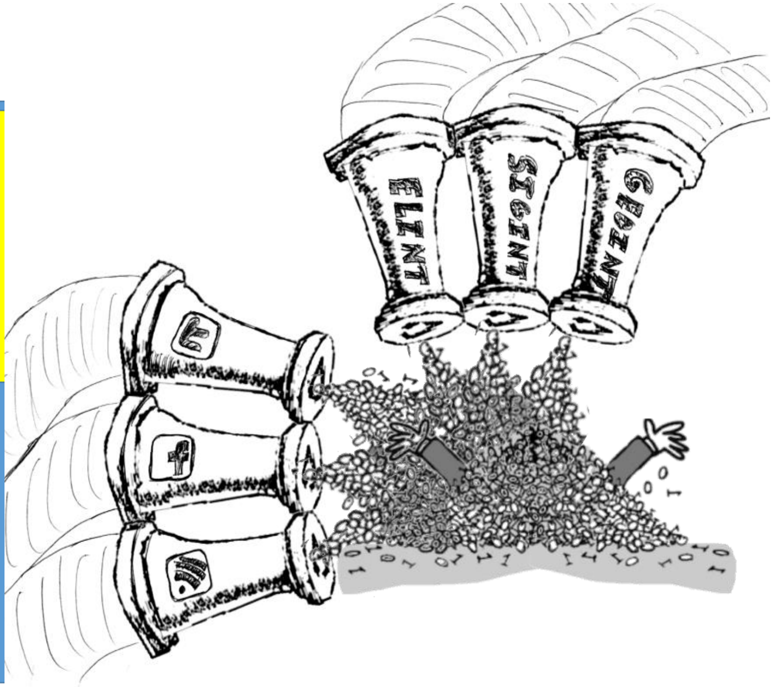
Threat Intelligence Analysis



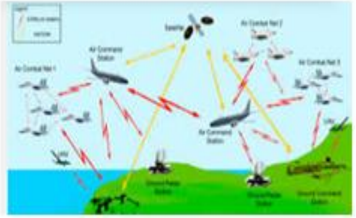
Cybersecurity

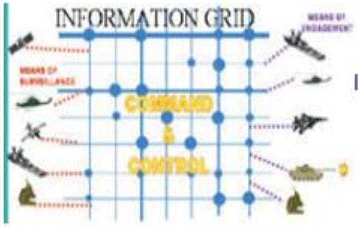
Situational Awareness

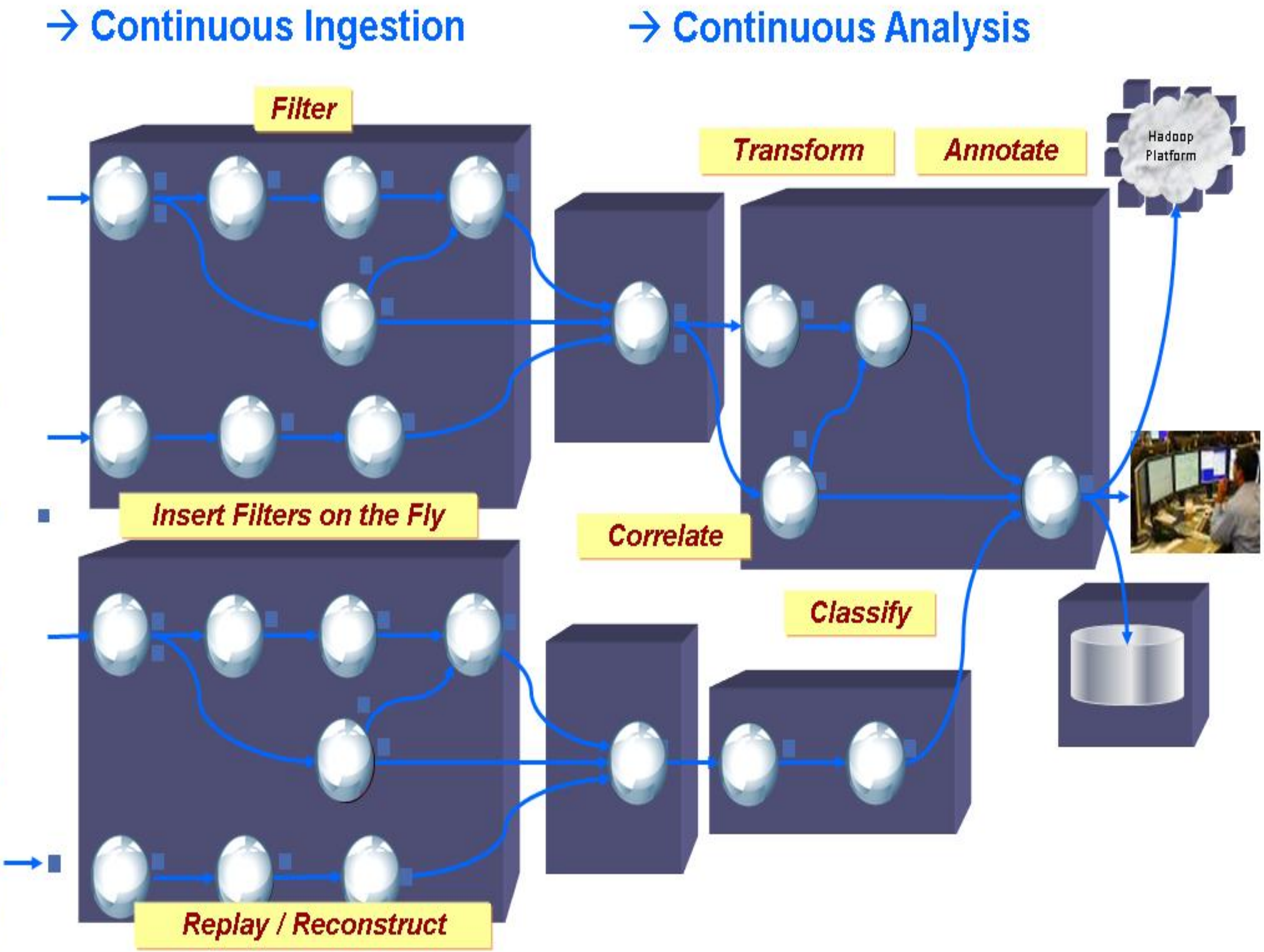
INTELLIGENCE
Traditional : HUMINT, SIGINT, etc.
Extended: OSINT, SOCMINT, etc.



Stream Processing







Predictive Modeling & Machine Learning

Big Data - Streams Processing

- Built in data connections and preparation for cyber data
- Integrate Predictive Models for threat detection
- Provides real time scoring and alerts

Machine Learning - Predictive Models

- Industry leading Predictive Analytics workbench
- Re-tune models to local, current data.
- Develop new models using machine based learning

Cyber Threat Visualization

- Distribute threat information across organization
- Develop dashboards and reports
- Mobile deployment to phones and tablets

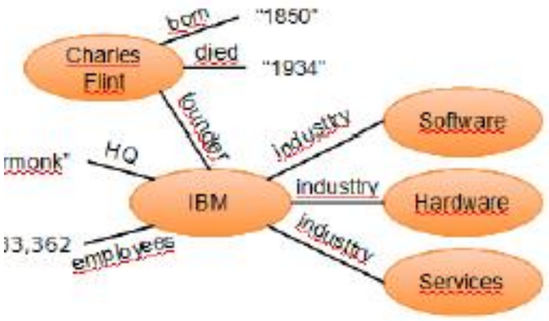
Improves Known Knowns (e.g., IPS)
Improves Known Unknowns (e.g., IDS)
Discovers Unknown Unknowns (e.g., Persistent Threats)

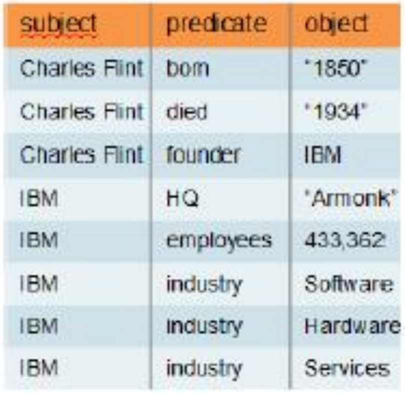
Graph Computing

Graph Database

Property Graph

Memory





subject	predicate	object
Charles Flint	born	"1850"
Charles Flint	died	"1934"
Charles Flint	founder	IBM
IBM	HQ	"Armonk"
IBM	employees	433,362
IBM	industry	Software
IBM	industry	Hardware
IBM	industry	Services

Related Information

Graph Analytics

Relation Graph

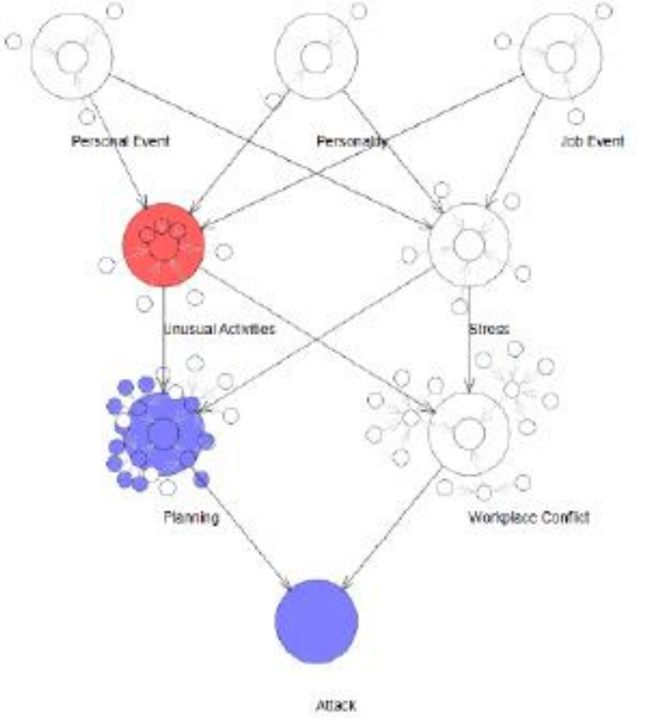
Perception

Contextual Analysis

Graphical Models

Reasoning Graph

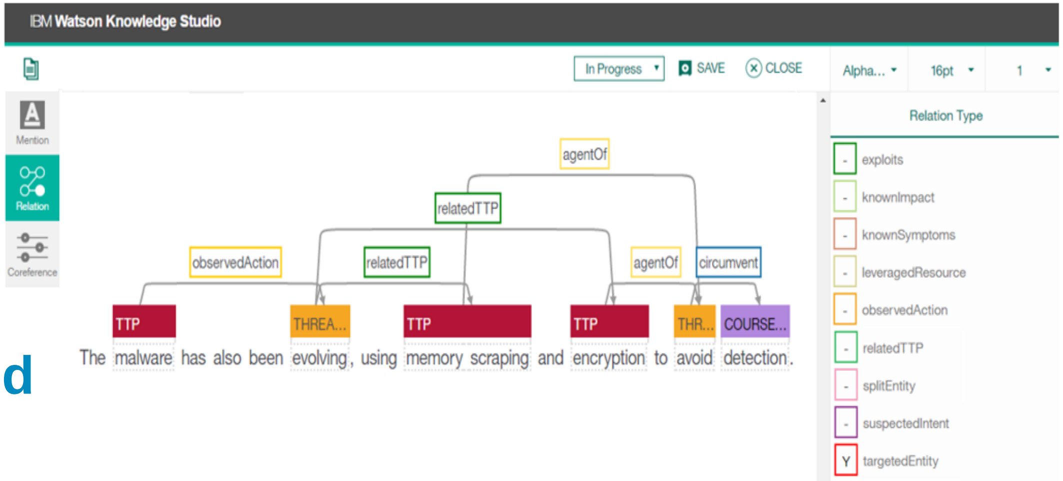
Intelligence

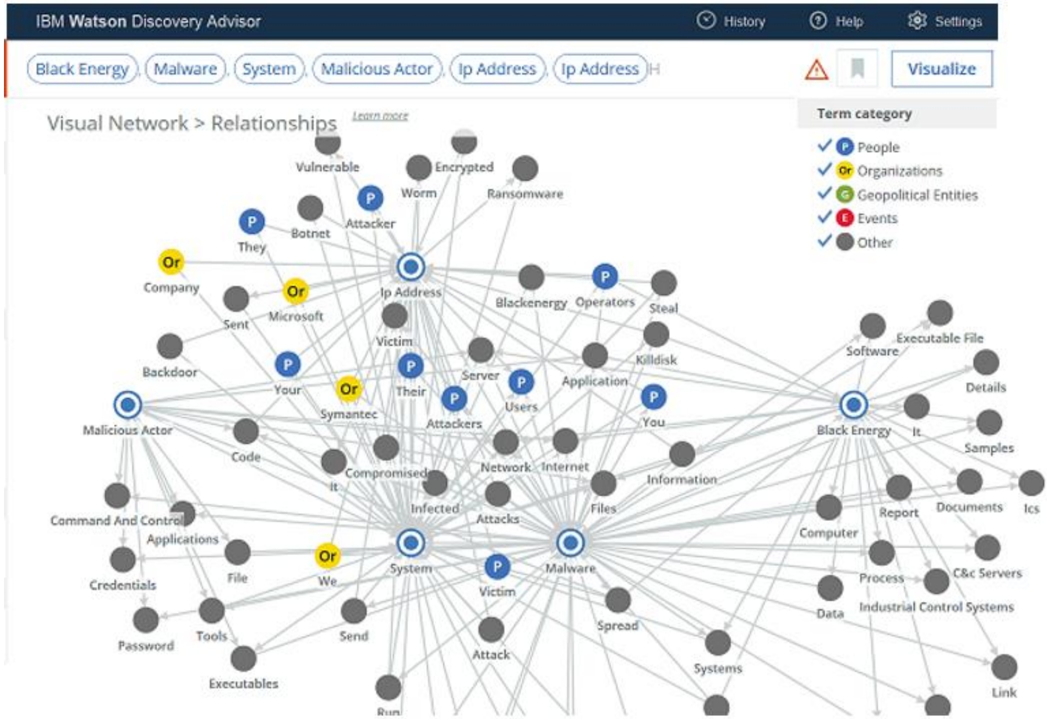


Machine Reasoning & Deep Learning

Information Extraction and Visualization

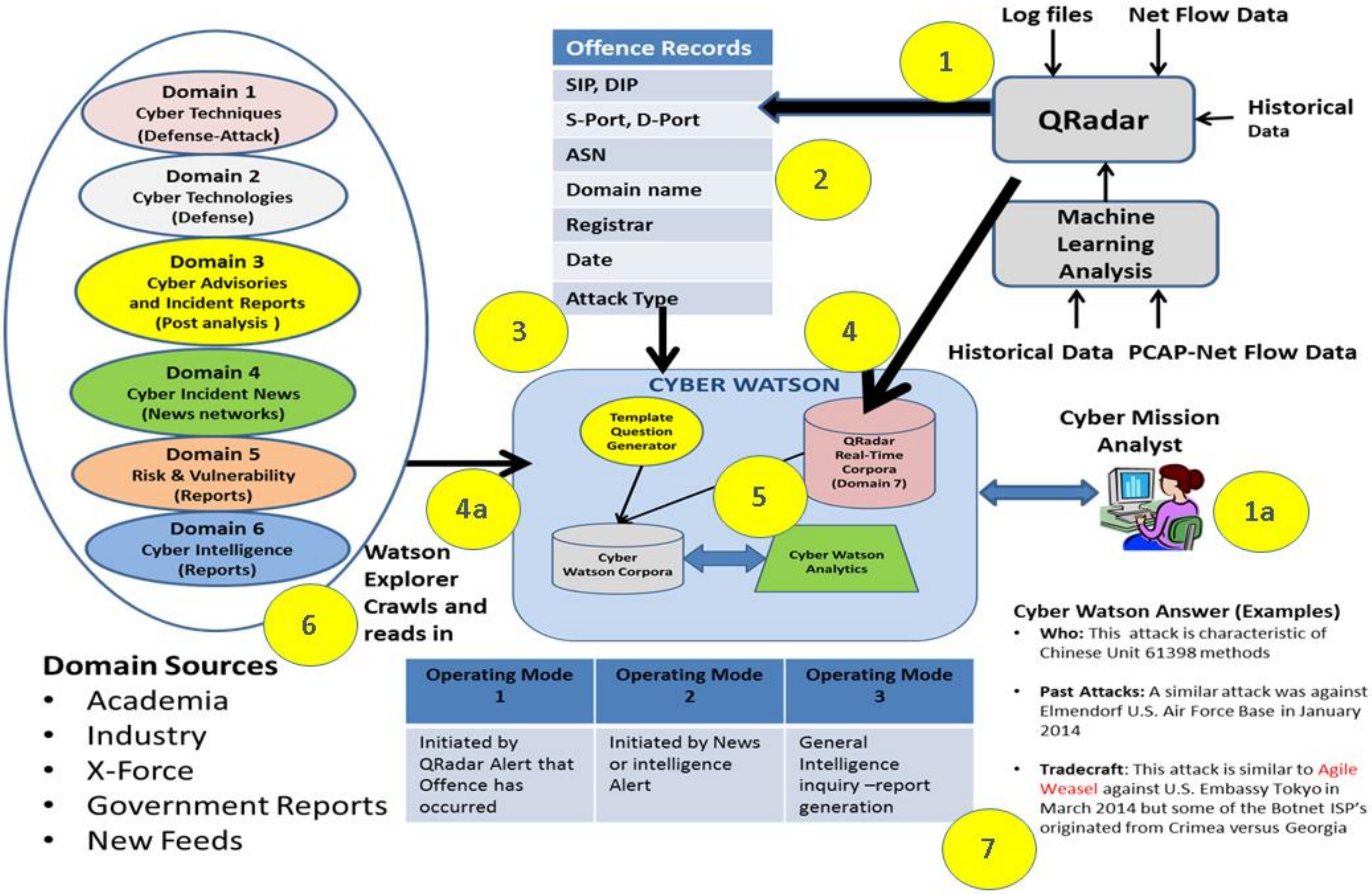
- Automated the process for extracting tacit information from unstructured text
- Use classification and detection models
- Ontology identifies real-world conceptual objects and relations between them





- Knowledge Graphs enable visualization and exploration between entities and relationships
- Show strength, nature & proximity of the relationship and interaction
- Exploit temporal, sequence, state, entry/exit criteria and other contextual views

Cognitive Analytics



Domain Sources

- Academia
- Industry
- X-Force
- Government Reports
- New Feeds

Operating Mode 1	Operating Mode 2	Operating Mode 3
Initiated by QRadar Alert that Offence has occurred	Initiated by News or intelligence Alert	General Intelligence inquiry –report generation

Cyber Watson Answer (Examples)

- **Who:** This attack is characteristic of Chinese Unit 61398 methods
- **Past Attacks:** A similar attack was against Elmendorf U.S. Air Force Base in January 2014
- **Tradecraft**: This attack is similar to Agile Weasel against U.S. Embassy Tokyo in March 2014 but some of the Botnet ISP's originated from Crimea versus Georgia

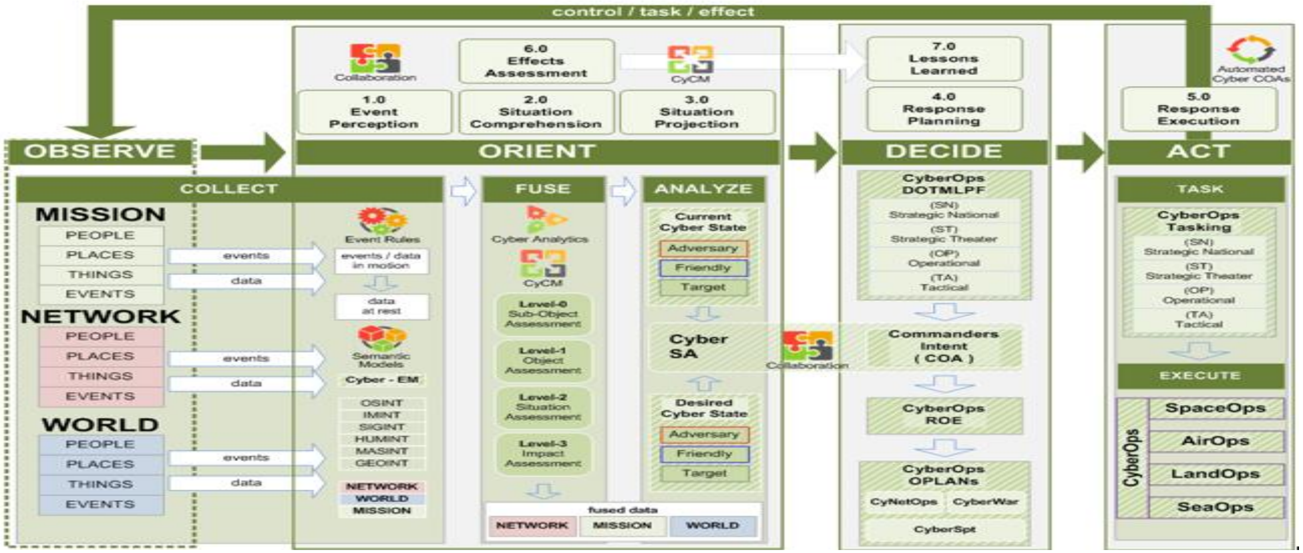
Decision Support Systems

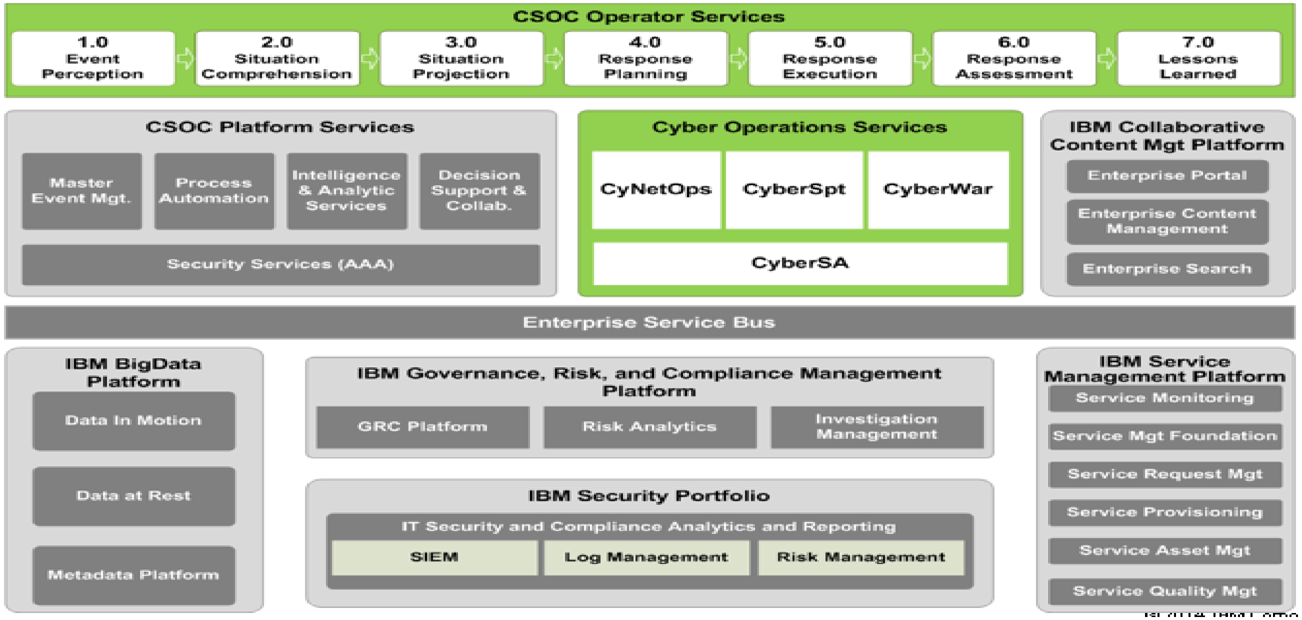
OODA Loop

Standard Operating Procedures

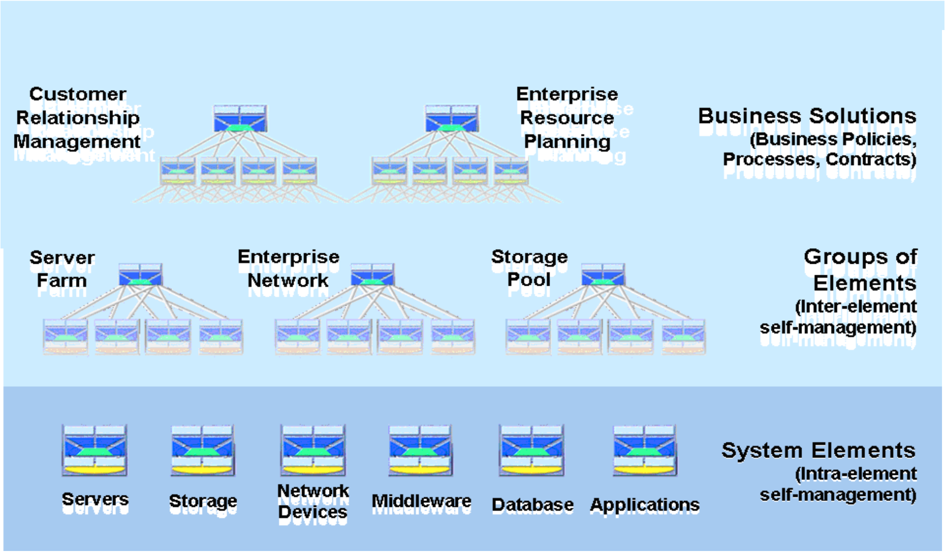
STANAGS

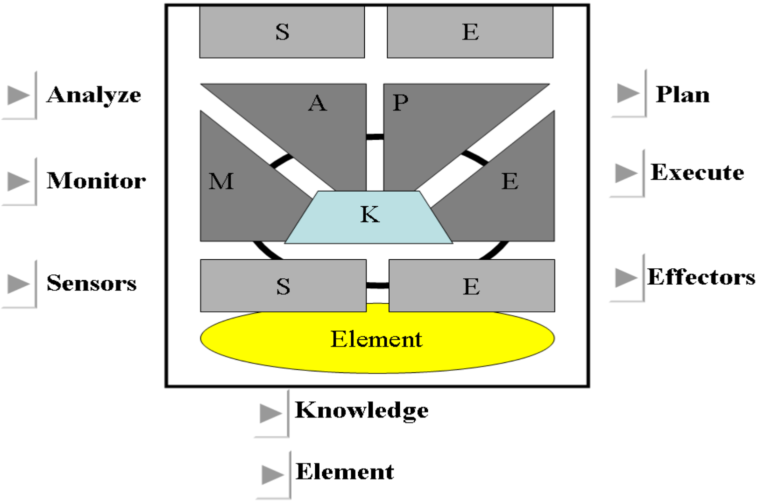
Cyber Informatics Support Cybernetics

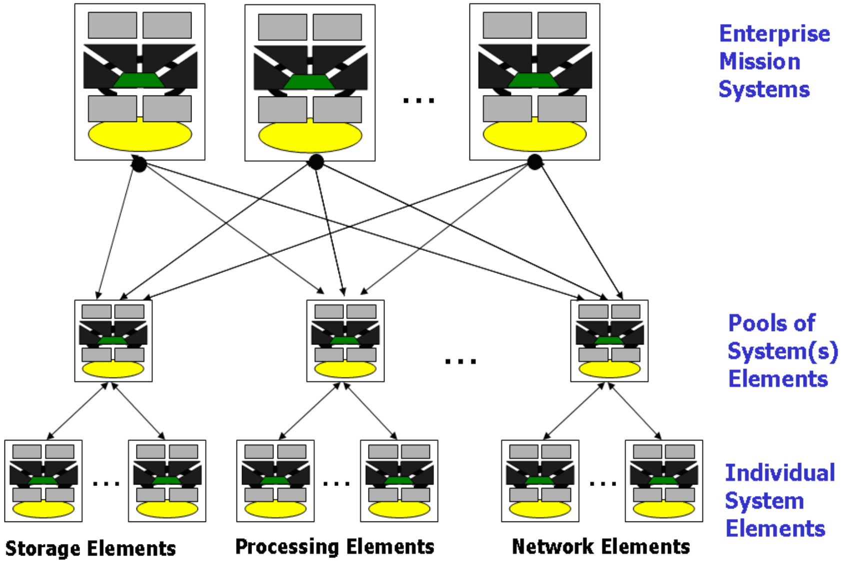




Autonomic Computing


Customer Relationship Management
Enterprise Resource Planning
Business Solutions
(Business Policies, Processes, Contracts)
Server Farm
Enterprise Network
Storage Pool
Groups of Elements
(Inter-element self-management)
Servers
Storage
Network Devices
Middleware
Database
Applications
System Elements
(Intra-element self-management)




...
Enterprise Mission Systems
...
Pools of System(s) Elements
...
...
...
Individual System Elements
Storage Elements
Processing Elements
Network Elements

Summary & Conclusions

- **OBSERVATION**: CyberSecurity challenges exacerbated by many modern threats, new assets to protect, and advances in technology that can (and are) being used neferiously. V = f(T,A)
- **RECOMMENDATION**: Extend CyberSecurity to incorporate Threat Intelligence Analysis and Situational Awareness information & analytics
- **RECOMMENDATION**: Exploit the many advances in Informatics (Predictive Modeling, Stochastic, Machine Learning, Graph Computing, Cognitive)
- **RECOMMENDATION**: Exploit advances in Cybernetics (Decision Support Systems & Autonomic Computing)

BUSINESS
INTERNATIONAL
MACHINES

As we embark on our second century...

Let's take a step back to reflect on lessons learned, celebrate innovations and reaffirm our ongoing commitment to progress.