Achieving IT Security Intelligence

By John W. Lainhart

IT security needs to be proactive—using cyber analytics and cognitive-based systems to ultimately achieve security intelligence. No longer can security programs rely on "if it's not broke, don't fix it"–the bad guys could already be inside your systems, stealing your data or probing to get in. Too many CIOs and CISOs are looking for jobs because they thought their systems and data were secure when, in fact, the opposite was true. Security programs need effective protection of valuable information and systems to prevent data breaches and to comply with the ever-increasing federal compliance requirements (e.g., FISMA, the Privacy Act, NIST, OMB mandates, FedRAMP, HIPAA/HITECH, etc.).

Security Challenges are Greater than Ever

With massive increases in data, mobile devices, and connections, security challenges are increasing in number and scope. They fall into three major categories: external threats, internal threats, and compliance requirements.

External Threats

The nation faces a proliferation of external attacks against major companies and government organizations. In the past, these threats have largely come from individuals working independently. However, these attacks have become increasingly more coordinated, and they are launched by groups ranging from criminal enterprises to organized collections of hackers to state-sponsored entities; attackers' motivations can include profit, prestige, or espionage.

These attacks target ever more critical organizational assets, including customer databases, intellectual property, and even physical assets that are driven by information systems. They have significant consequences, resulting in IT, legal, and regulatory costs. Many of these attacks take place slowly over time, masked as normal activity. The threat vector known as advanced persistent threat (APT) requires specialized continuous monitoring methods to detect threats and vulnerabilities prior to breaches or loss of sensitive data.

Internal Threats

In many situations, breaches in information security are not perpetuated by external parties but by insiders. Insiders today can be employees, contractors, consultants, and even partners and service providers. These breaches range from careless behavior and administrative mistakes (such as giving away passwords to others, losing backup tapes or laptops, or inadvertently releasing sensitive information) to deliberate actions taken by disgruntled employees. These actions can lead to harm as dangerous as external attacks, if not more so.

Compliance Requirements and Effective Protection

Public sector enterprises face a steadily increasing number of federal, industry, and local mandates related to security, each of which have their own standards and reporting requirements. These many mandates include FISMA, the Privacy Act, NIST standards and special publications, OMB mandates, FedRAMP, HIPAA/HITECH, Sarbanes-Oxley, various state privacy/data breach laws, IRS 1075, SSAE 16, COBIT®, various ISO/IEC international standards, EU privacy directives, etc. Complying with these requirements often takes a significant amount of time and effort to prioritize issues, develop appropriate policies and controls, and monitor compliance.

To address external, internal, and compliance challenges through a proactive approach, four key areas must be addressed to protect an organization's systems and data:

- Security architecture effectiveness
- Critical data protection
- Security compliance
- Holistic security program

John W. Lainhart is Cybersecurity Fellow at IBM Center for The Business of Government.

Security Architecture Effectiveness focuses on rapidly accessing vulnerabilities in the security architecture and developing a prioritized roadmap to strengthen cyber protection by plugging security gaps and meeting policy expectations.

Critical Data Protection focuses on rapidly accessing the data architecture and shortfalls in tracking and protecting critical data. Prioritized action plans can reshape data architecture for more focused security protection and improved continuous monitoring.

Security Compliance focuses on rapidly accessing compliance gaps and establishing a roadmap to prioritize and achieve compliance.

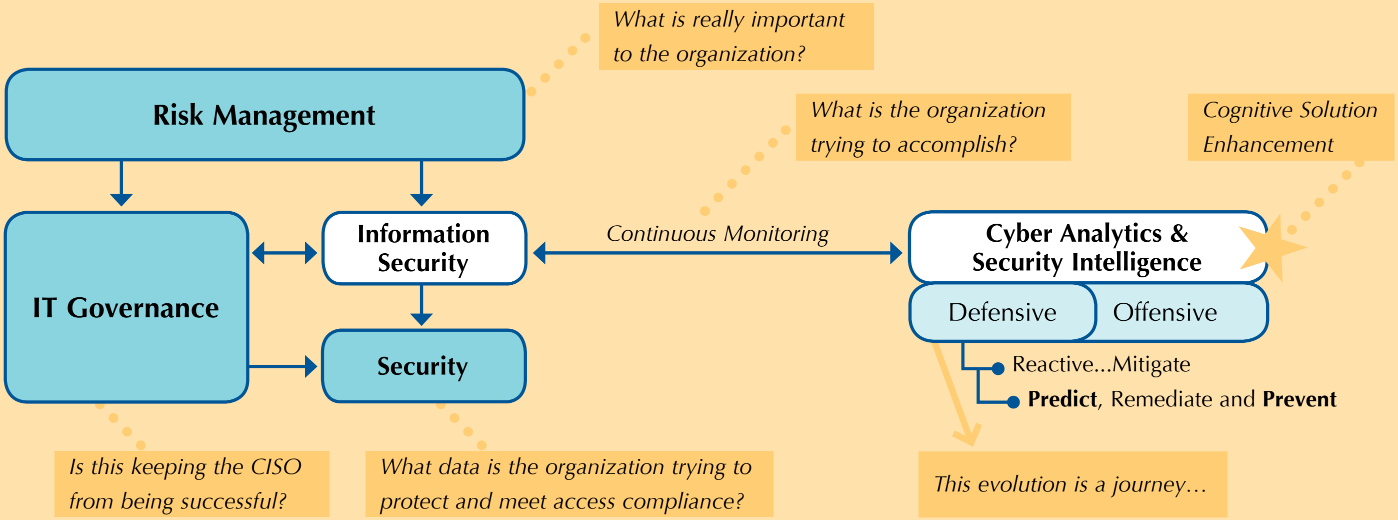
Effectively implementing the first three areas above can enable the establishment of a **Holistic Security Program** that addresses risk management and IT governance:

- Risk identifies critical business processes that are most import to an agency's mission success, as well as threats and vulnerabilities that can impact critical business processes.

- Information technology (IT) governance is a key enabler of successful cybersecurity protection. Consistent and standardized security and privacy processes and technology configurations support protection at a lower cost. These types of relationships are depicted below.

The graphic below demonstrates how a holistic security program focuses on protection through continuous monitoring of systems and data. This involves moving from a more common defensive-reactive approach to a defensive-proactive (predictive) approach, using cyber analytics to foster "security intelligence," which also protects privacy.

A Holistic Security Program Approach


What is really important to the organization?
Risk Management
What is the organization trying to accomplish?
Cognitive Solution Enhancement
IT Governance
Information Security
Continuous Monitoring
Cyber Analytics & Security Intelligence
Defensive
Offensive
Security
Reactive...Mitigate
Predict, Remediate and **Prevent**
Is this keeping the CISO from being successful?
What data is the organization trying to protect and meet access compliance?
This evolution is a journey…

Continuous monitoring is now required by OMB and NIST mandates, and it can be supplemented using cyber analytics to proactively highlight risks and identify, monitor, and address threats. As enterprises bolster their security defenses, predictive analytics plays an increasingly important role (see the figure below). Enterprises can conduct sophisticated correlations to detect advanced persistent threats while implementing governance and automated enterprise risk processes—critical building blocks for enabling security intelligence. This includes the ability to:

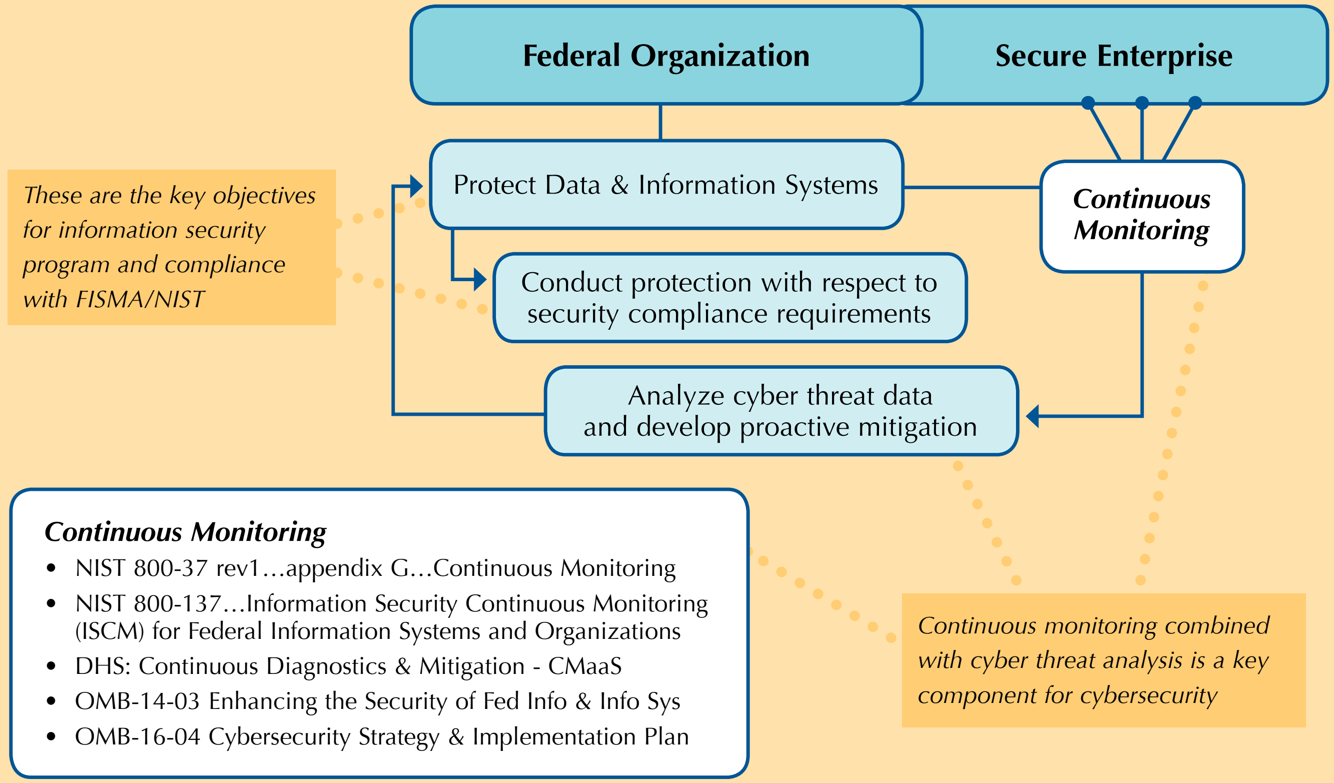
- Identify previous breach patterns and outside threats to predict potential areas of attack.
- Analyze insider behavior to identify patterns of potential misuse.
- Monitor the external environment for potential security threats.

Continuous monitoring, combined with cyber analytics via security intelligence, can provide key cybersecurity capabilities, as depicted in the graphic below. Continuous monitoring and analysis of cyber threat-related data sources (e.g., DNS, Netflow, query results) provides the needed context for the fusion of data that can be analyzed using tools to produce actionable, meaningful, and timely information for CISOs and CIOs to address the most important issues affecting their agency, and to deter and prevent cyber threats.

Using cyber analytics to proactively highlight risks and identify, monitor, and address threats and vulnerabilities helps to achieve predictive and preventive cybersecurity capabilities.

However, cyber analytics can also be greatly enhanced using cognitive-based systems to build knowledge, learn and understand natural language, and reason and interact more naturally with human beings. They are also able to put content into context with confidence-weighted responses and supporting evidence. They can quickly identify new patterns and insights. Specifically, cognitive solutions have these three critical capabilities that are needed to achieve security intelligence:

Protecting Data and Systems–Primary Objective

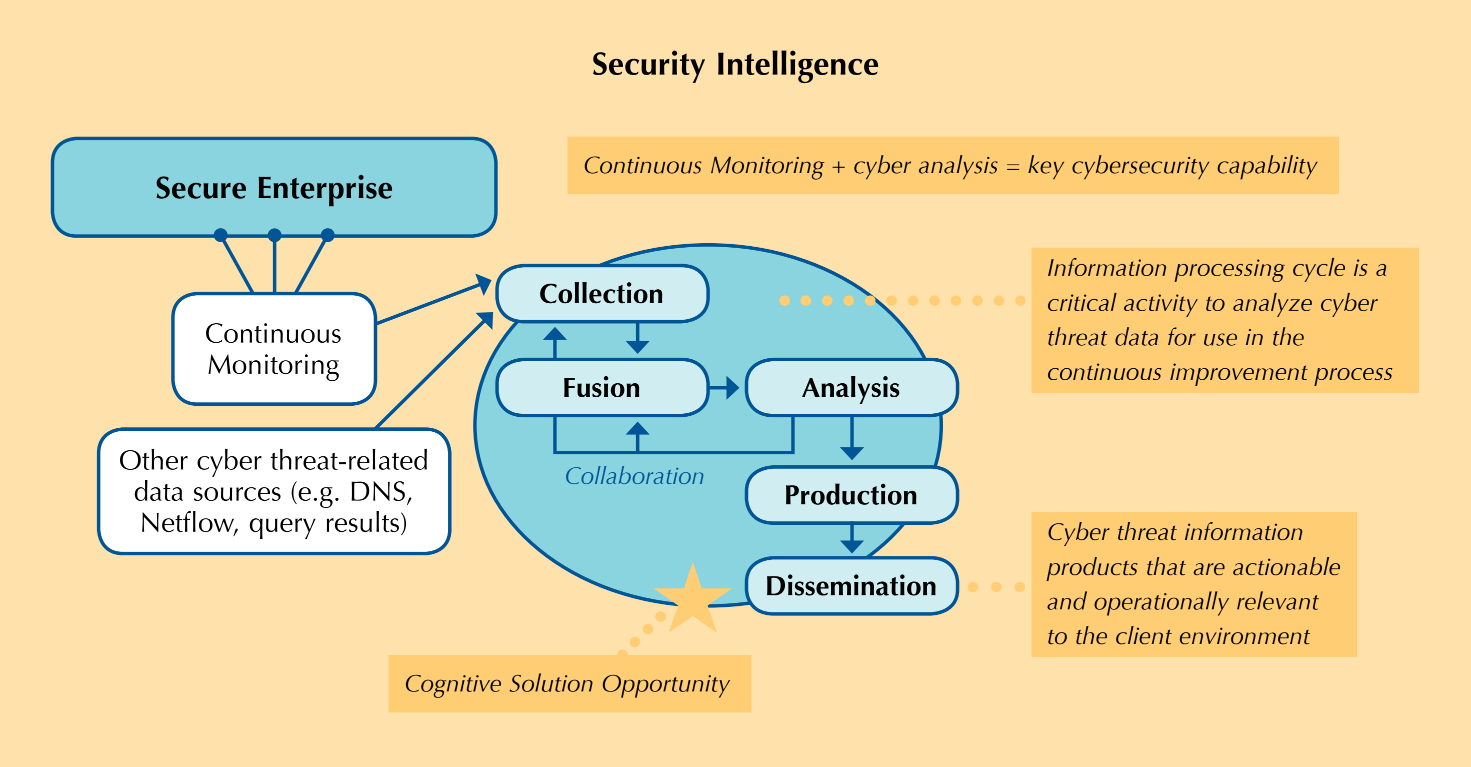

Federal Organization
Secure Enterprise
Protect Data & Information Systems
Continuous Monitoring
Conduct protection with respect to security compliance requirements
Analyze cyber threat data and develop proactive mitigation

These are the key objectives for information security program and compliance with FISMA/NIST

Continuous Monitoring

- NIST 800-37 rev1…appendix G…Continuous Monitoring
- NIST 800-137…Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- DHS: Continuous Diagnostics & Mitigation - CMaaS
- OMB-14-03 Enhancing the Security of Fed Info & Info Sys
- OMB-16-04 Cybersecurity Strategy & Implementation Plan

Continuous monitoring combined with cyber threat analysis is a key component for cybersecurity


Security Intelligence
Continuous Monitoring + cyber analysis = key cybersecurity capability
Secure Enterprise
Continuous Monitoring
Other cyber threat-related data sources (e.g. DNS, Netflow, query results)
Collection
Fusion
Analysis
Collaboration
Production
Dissemination
Information processing cycle is a critical activity to analyze cyber threat data for use in the continuous improvement process
Cyber threat information products that are actionable and operationally relevant to the client environment
Cognitive Solution Opportunity

1. **Engagement.** These systems provide expert assistance by developing deep domain insights and presenting the information in a timely, natural and usable way.

2. **Decision.** These systems have decision-making capabilities. Decisions made by cognitive systems are evidence-based and continually evolve based on new information, outcomes, and actions.

3. **Discovery.** These systems can discover insights that perhaps could not be discovered otherwise. Discovery involves finding insights and connections and understanding the vast amounts of information available.

Thus, agency senior executives involved in cybersecurity need to move from a basic to an optimized level of security intelligence.

Achieving cybersecurity protection is a way to preserve mission success while achieving key objectives for the agency's security program. Government needs to move from a basic (manual and reactive) to an optimized (automated and proactive) posture to secure critical systems and valuable information through security intelligence. ◘