Fusion Center Concept

Introductions

Sunny Jassal has 20+ years of combined experience in IT and Cybersecurity, leading highly technical teams across various sectors. He is currently the Interim Chief Information Officer (CIO) at British Columbia Institute of Technology (BCIT) responsible for all aspects of IT and Cybersecurity.

Prior to his appointment as Interim CIO, Sunny served as Director of Cybersecurity, BCIT for four years where he provided leadership across Cybersecurity and IT Risk Management. Sunny was instrumental in building a team and leading key technology and risk initiatives at the institute. Sunny has special interests in Cybersecurity and leads by the principle of 'security by design'.

Sunny holds a B.Tech in Technology Management from BCIT along with top industry certifications like, Certified Chief Information Security Officer (CCISO), Certified Information Security Manager (CISM), Certified Data Privacy Solutions Engineer (CDPSE) and Systems Security Certified Practitioner (SSCP).

Hardeep Mehrotara has 20+ years of experience in IT and Cybersecurity, working in a senior leadership roles for public and private organizations. He is currently the Director of Information Security & Enterprise Architecture at Concert Properties responsible for IT and OT security.

Hardeep has significant background in building security programs and leading high-performance teams. He has been featured on various TV outlets and currently serves on program advisory committees for various higher-Eds. Hardeep also serves in the Canadian Forces as an officer responsible for cyber force development, cyber missions, and training.

Hardeep holds an mMBA from McGill, Management of Technology from MIT, and Honors Degree in Computer Crime & Forensics from BCIT. He has a strong background in law enforcement and collaborated and co-authored technical publications at the Centre of Internet Security and World Economic Forum.

Disclaimer

The views and opinions expressed during this presentation and on the following slides are solely those of the presenter(s) and do not necessarily represent official policy or position of the presenter(s) employer’s or of its stakeholders.

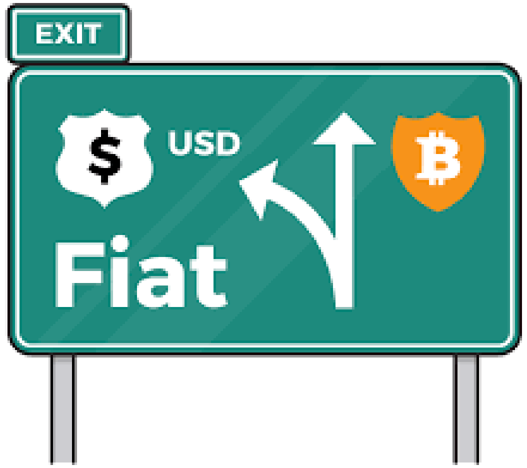
Panel Reflection

Session 1 - Fusion Center Model Panel Sessions: Accelerating convergence underway between cybersecurity, fraud and anti-money laundering.

It is needless to say due to yesterday’s silos between cybersecurity, fraud and anti-money laundering, detection of cybersecurity related fraud requires a special multi-disciplinary and innovative playbook built on convergence of the silos in order to establish a clear strategic enterprise vision. This vision and fusion is tomorrow’s fusion center model - future ready and resilient!

Problem Statement

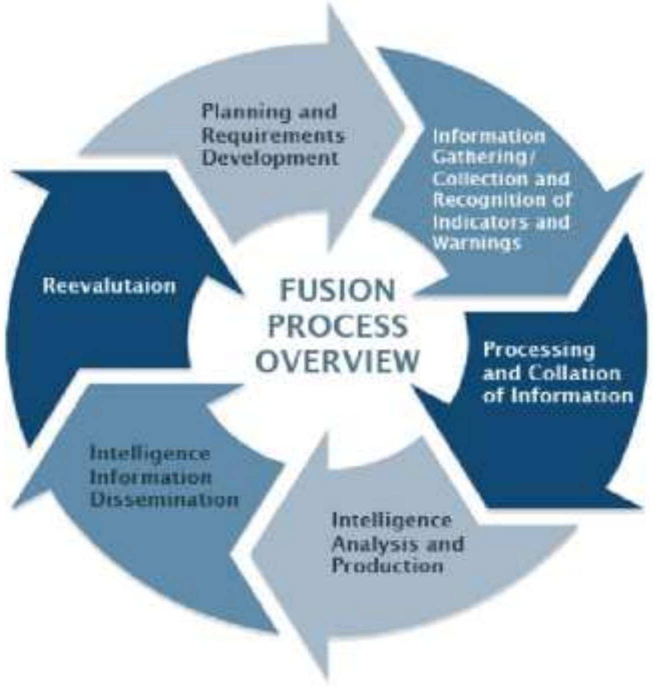
Our modern way of life, growing interconnected devices, data and privacy, disruptions in technology and fintech, critical infrastructure, growing geo-political and nation-state threats, has challenged our traditional approach to threat detection and response. Speed to change and agility to move quickly are not human strengths.



What is a Fusion Concept

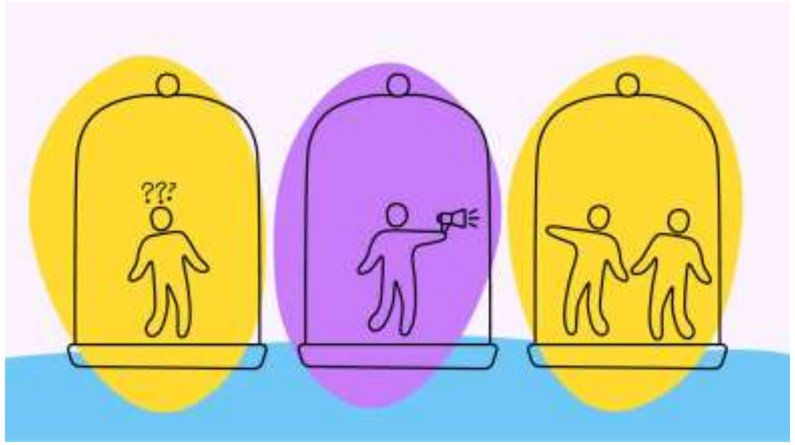
- A collaborative model where individuals from different risk areas come together with a common purpose to achieve a coordinated response.

- “Turning Information and Intelligence Into Actionable Knowledge.” - ***Homeland Security***


FUSION PROCESS OVERVIEW
Planning and Requirements Development
Information Gathering/ Collection and Recognition of Indicators and Warnings
Processing and Collation of Information
Intelligence Analysis and Production
Intelligence Information Dissemination
Reevalutaion

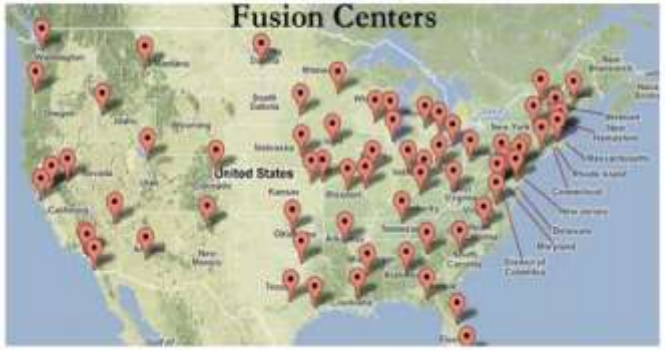
Key Challenges with Cyber and Fraud

- Traditionally Siloed
- More reactive and less proactive
- Complexity in organizational structures and design
- Difficult to detect coordinated and advanced threats and methods
- Focus on manual workflows with limited automation
- Lack of consistent and repeatable processes increasing response and recovery times.
- Overall lack of resiliency due to human scalability



Where are Fusion Centers used?

Law Enforcement & Intelligence



National Fusion Center Association map of fusion centers nationwide. Does not include all fusion centers.

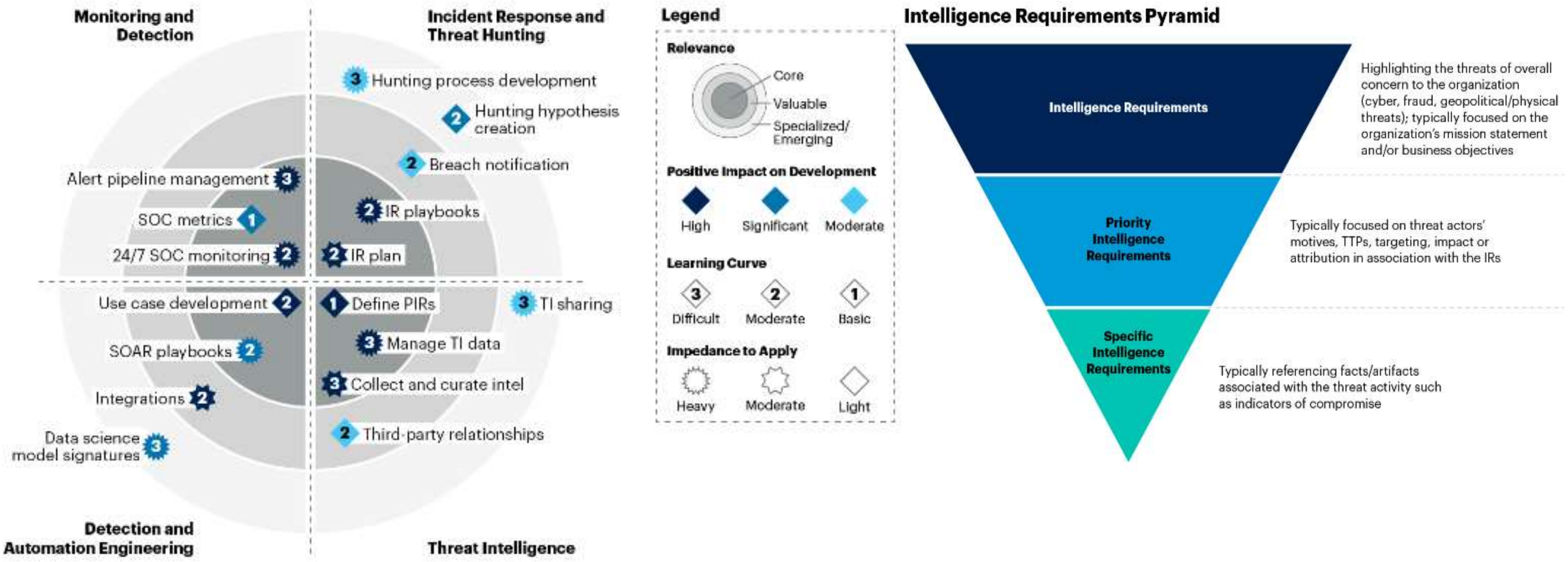
Financial

Cyber

Benefits of Fusion Concept

- Address multi-layered threats
- Integrated Approach
- Shared visibility and shared cost
- Faster and efficient information sharing across various groups
- Provide a unique perspective on a threat
- Actionable Knowledge
- Speed and Agility
- Coordinated Response

SOC Capabilities



Monitoring and Detection

- Alert pipeline management 3
- SOC metrics 1
- 24/7 SOC monitoring 2

Incident Response and Threat Hunting

- 3 Hunting process development
- 2 Hunting hypothesis creation
- 2 Breach notification
- 2 IR playbooks
- 2 IR plan

Detection and Automation Engineering

- Use case development 2
- SOAR playbooks 2
- Integrations 2
- Data science model signatures 3

Threat Intelligence

- 1 Define PIRs
- 3 TI sharing
- 3 Manage TI data
- 3 Collect and curate intel
- 2 Third-party relationships

Legend

Relevance

Core

Valuable

Specialized/ Emerging

Positive Impact on Development

High · Significant · Moderate

Learning Curve

3 Difficult · 2 Moderate · 1 Basic

Impedance to Apply

Heavy · Moderate · Light

Intelligence Requirements Pyramid

Intelligence Requirements: Highlighting the threats of overall concern to the organization (cyber, fraud, geopolitical/physical threats); typically focused on the organization's mission statement and/or business objectives

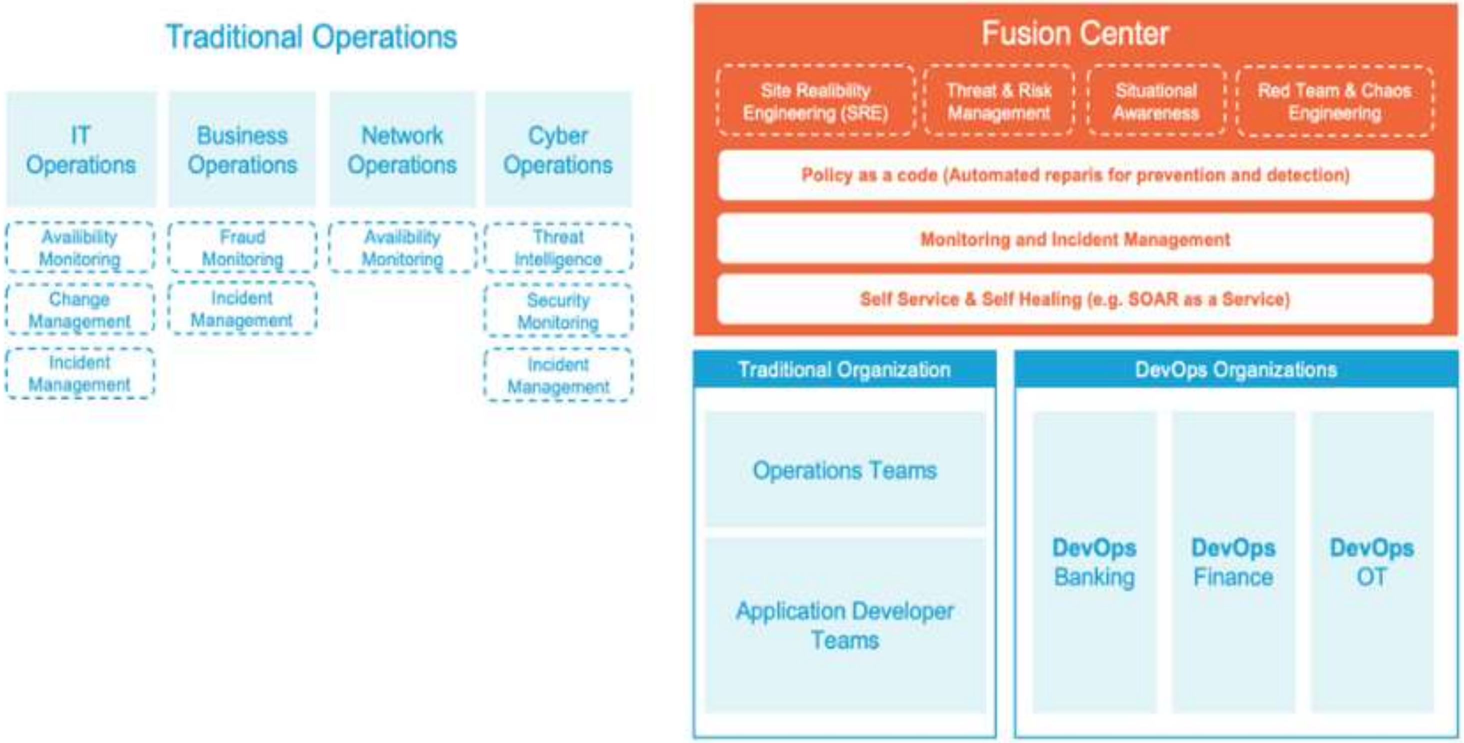
Priority Intelligence Requirements: Typically focused on threat actors' motives, TTPs, targeting, impact or attribution in association with the IRs

Specific Intelligence Requirements: Typically referencing facts/artifacts associated with the threat activity such as indicators of compromise

Source: Gartner

Challenges with SOCs

- Large-scale cyber heists like the 2016 Bangladesh Bank robbery could have been avoided by a more integrated exchange of information
- ATM Cash out attacks are a combination of physical, cyber and fraud.
- SOCs are mainly focused on detection and response.
- Speed and agility is critical in effective detection and response.
- Automation is not always the focus or DevOps teams are not embedded.

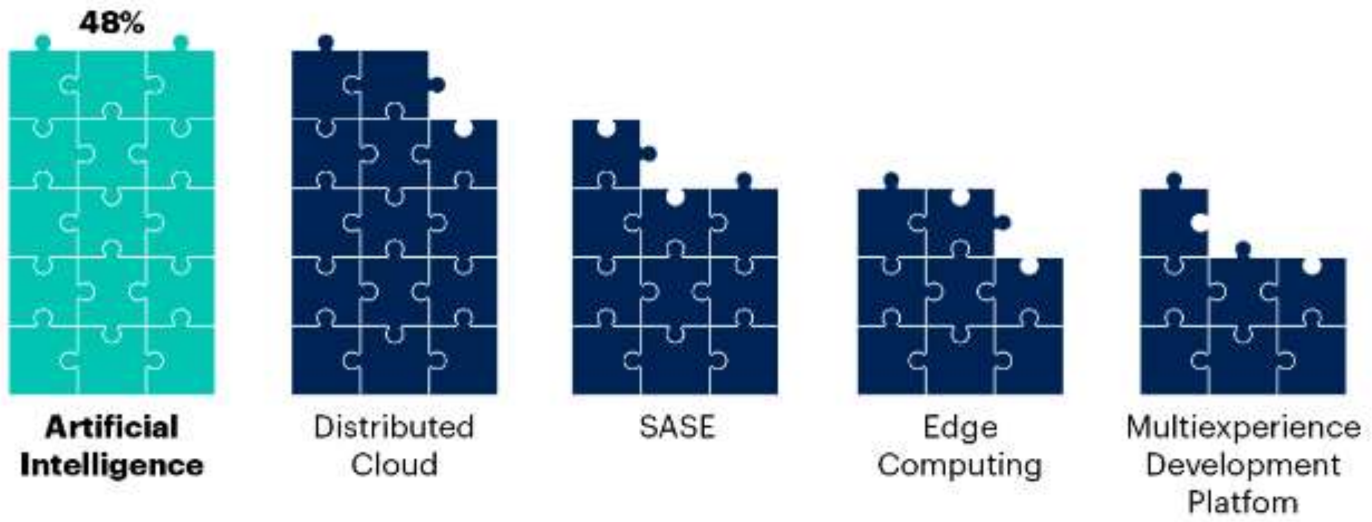


AI Opportunities

- Effective AI Management necessitates forging new partnerships
- Overcome Morale and Human burnout
- Overcome Insider Threat Management
- Speed and Agility is critical to establishing resilience

AI solutions are the top emerging technology to be deployed or close to deployment across enterprises ...

Emerging Technologies Deployed or Planned to Deploy in Next 12 Months

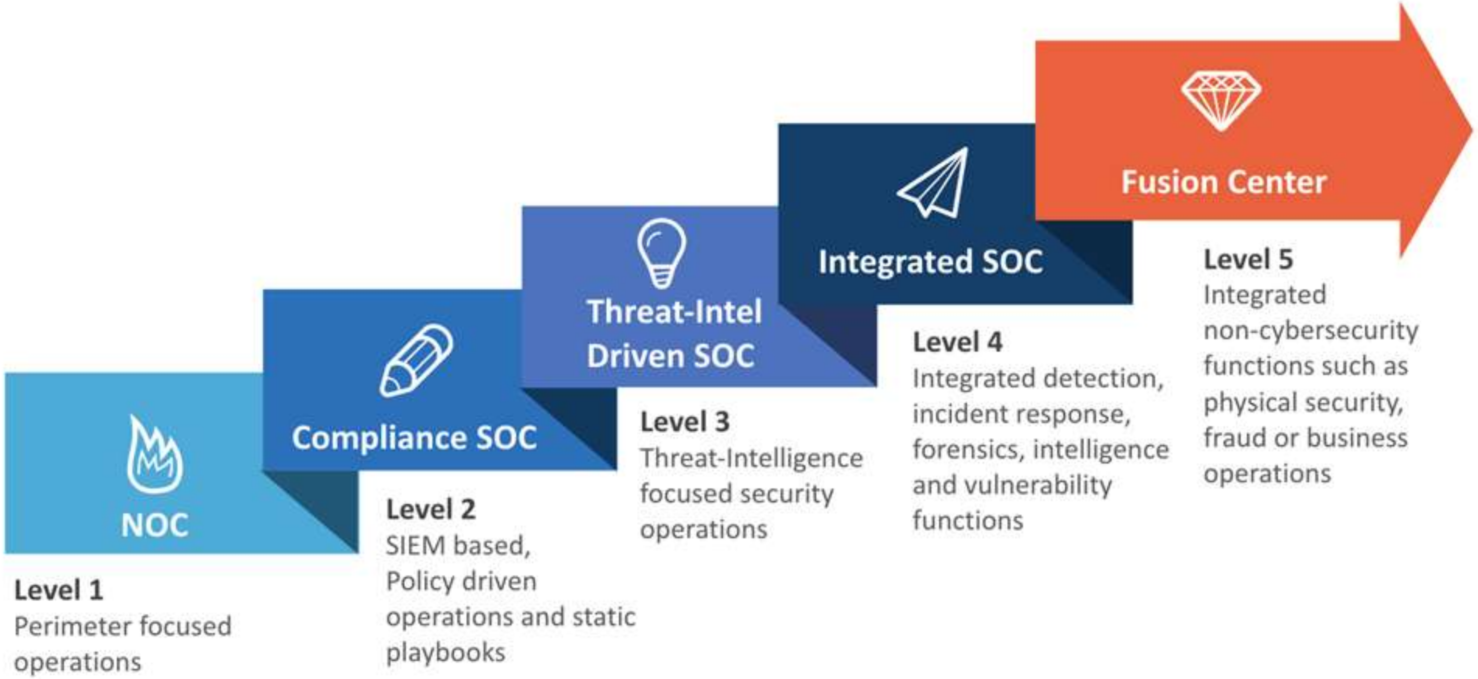


n = 2186 CIOs and technology executives

Source: 2023 Gartner CIO and Technology Executive Survey

Fusion Center evolution

- SOCs are becoming more complex with the evolution of business risk
- Outsourcing pieces of SOC capabilities adds to complexity
- Fusion concept integrates business operational capabilities bringing fraud, privacy, physical security and enterprise risk management together in a SOC
- Coordinated threat response enhancing business resilience



Level 1
Perimeter focused operations

Level 2
SIEM based, Policy driven operations and static playbooks

Level 3
Threat-Intelligence focused security operations

Level 4
Integrated detection, incident response, forensics, intelligence and vulnerability functions

Level 5
Integrated non-cybersecurity functions such as physical security, fraud or business operations

Benefits of Cyber Fusion Centers

Unifies security operations

Allow enterprises to bring cybersecurity and related risk operations under one unit.

Offers advanced-level security

Drives an unprecedented level of threat visibility, intelligence and collaboration across security units and provides advanced-level security bolstering expert-driven and security intelligence response.

Helps in faster decision making

Help organizations make faster security decisions due to the high level of collaboration and intelligence sharing the center offers.

Helps organizations to understand threat situations in real-time

A cyber fusion-based strategy enables firms to better understand and assess the threat environment in real time, by giving them more visibility into the actions and strategies of their attackers.

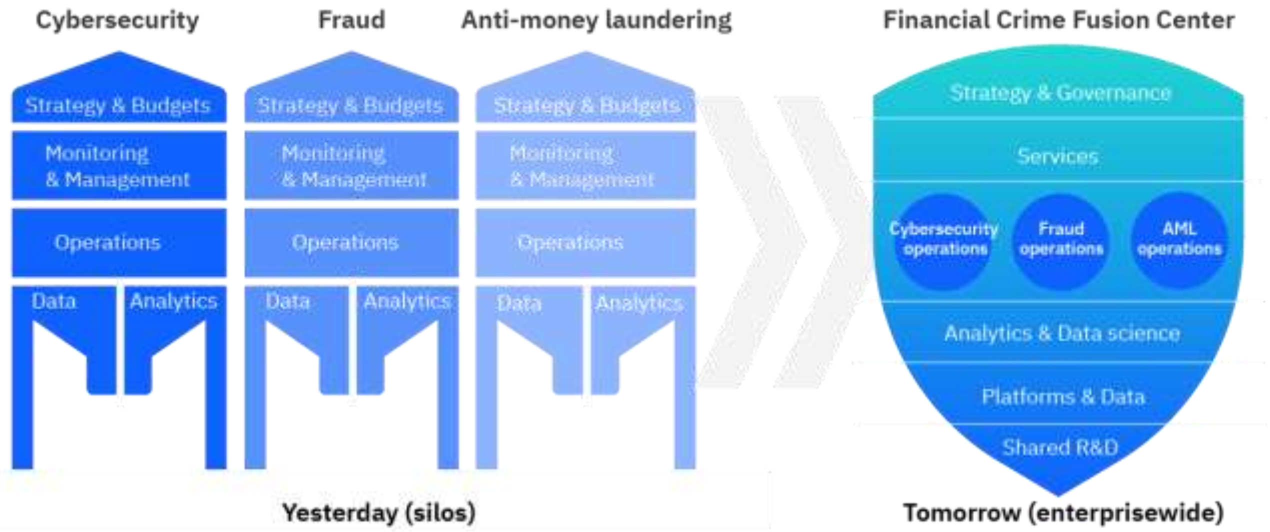
Responsibilities of a Fusion Center

- **Threat Intelligence -** Tactical, operational, and strategic intelligence
- **Analytics -** Analyzing operational and threat data, including user and entity behavior analytics
- **Threat Detection -** Identifying threats through alerts and security tools
- **Incident Response -** Responding as quickly as possible to the identified threats, breaches, and attacks
- **Security orchestration, automation and response (SOAR) -** SOAR enables security teams to handle incidents with automated workflows.
- **Governance & Compliance -** Ensuring all IT and security activities align to regulations and compliance concerns
- **Threat Hunting -** Locating and remediating threats not detected through alerts
- **Fraud Detection**
- **Privacy Breach Response**
- **Business Continuity**
- **Anti-Money-Laundering (AML)**
- **Physical Security**

Add Additional layers and departments to enhance coordination and response

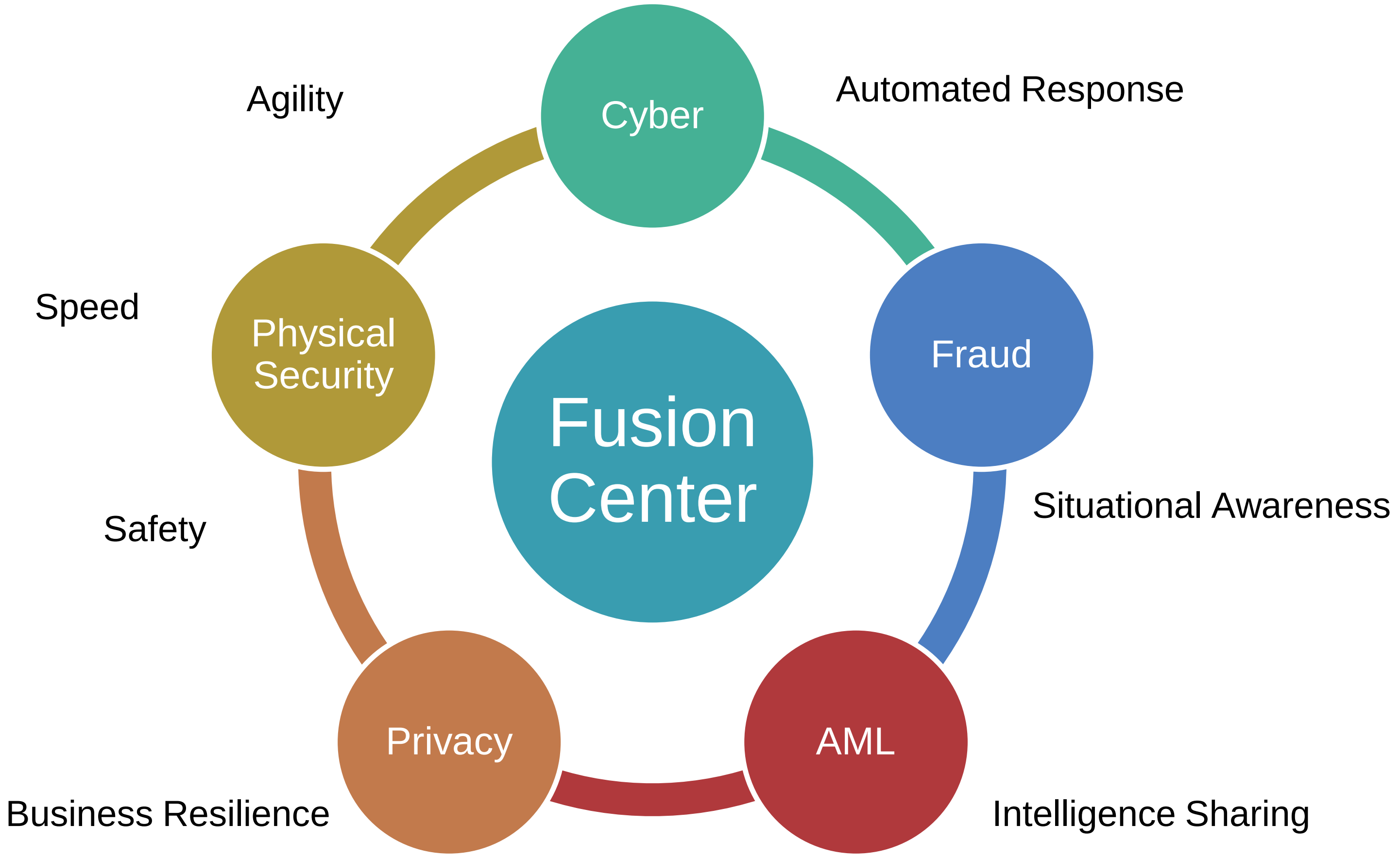
Commonalities between Cyber & Fraud Incident Playbooks with Fusion Models

- Transactions originating from suspicious countries.
- Detect an excessive number of transactions in a short period.
- Detect outlier transactions by value.
- Detect account changes with subsequent successful transactions.
- Detect multiple account login denials followed by authorization.
- Detect behavioural activity followed by transactional activity.



IBM Institute for Business Value

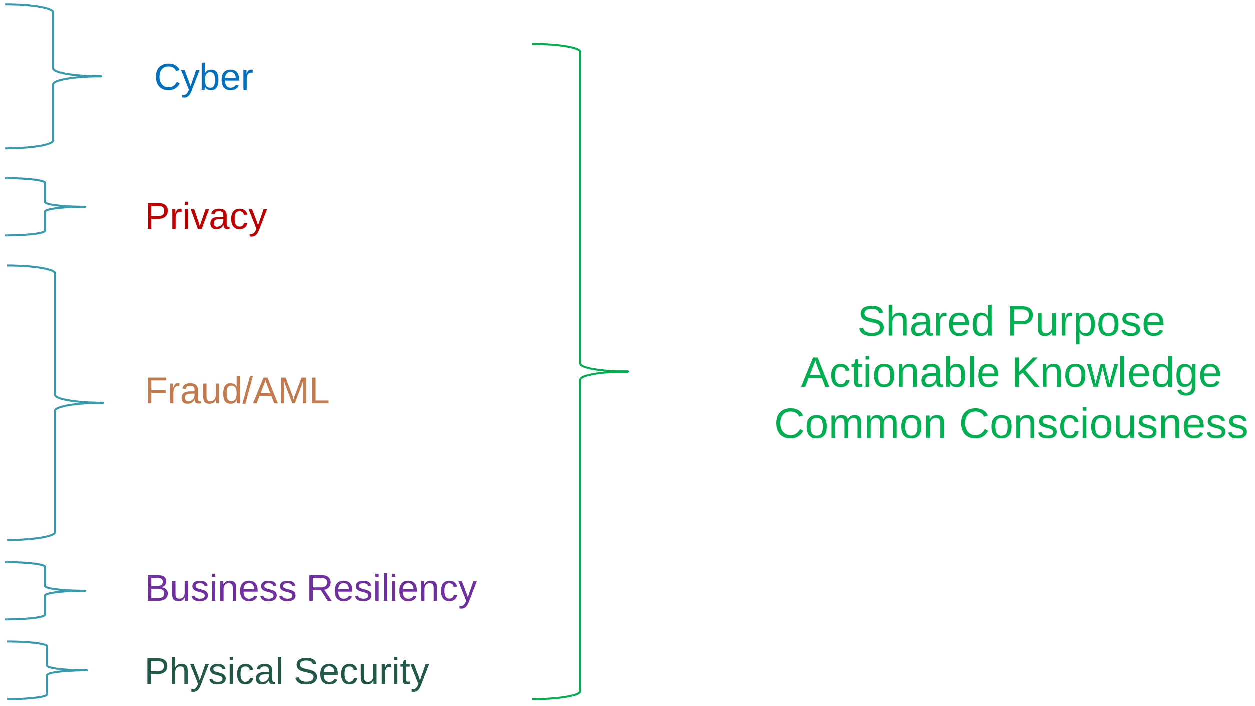
Future of Fusion Centers



Turning Information and Intelligence Into Actionable Knowledge

Fusion Center Approach – Exercise

1. An employee's credentials are stolen.
2. Malware is installed on the company network.
3. Finance department credentials compromised.
4. Personal information of customers is stolen.
5. Funds are stolen from company's bank's account.
6. Funds are routed to a third-party bank in another country.
7. Withdrawals are made through multiple transactions.
8. Millions of dollars are stolen.
9. Ransomware is deployed.
10. Insider Threat & Law Enforcement



Cyber

Privacy

Fraud/AML

Business Resiliency

Physical Security

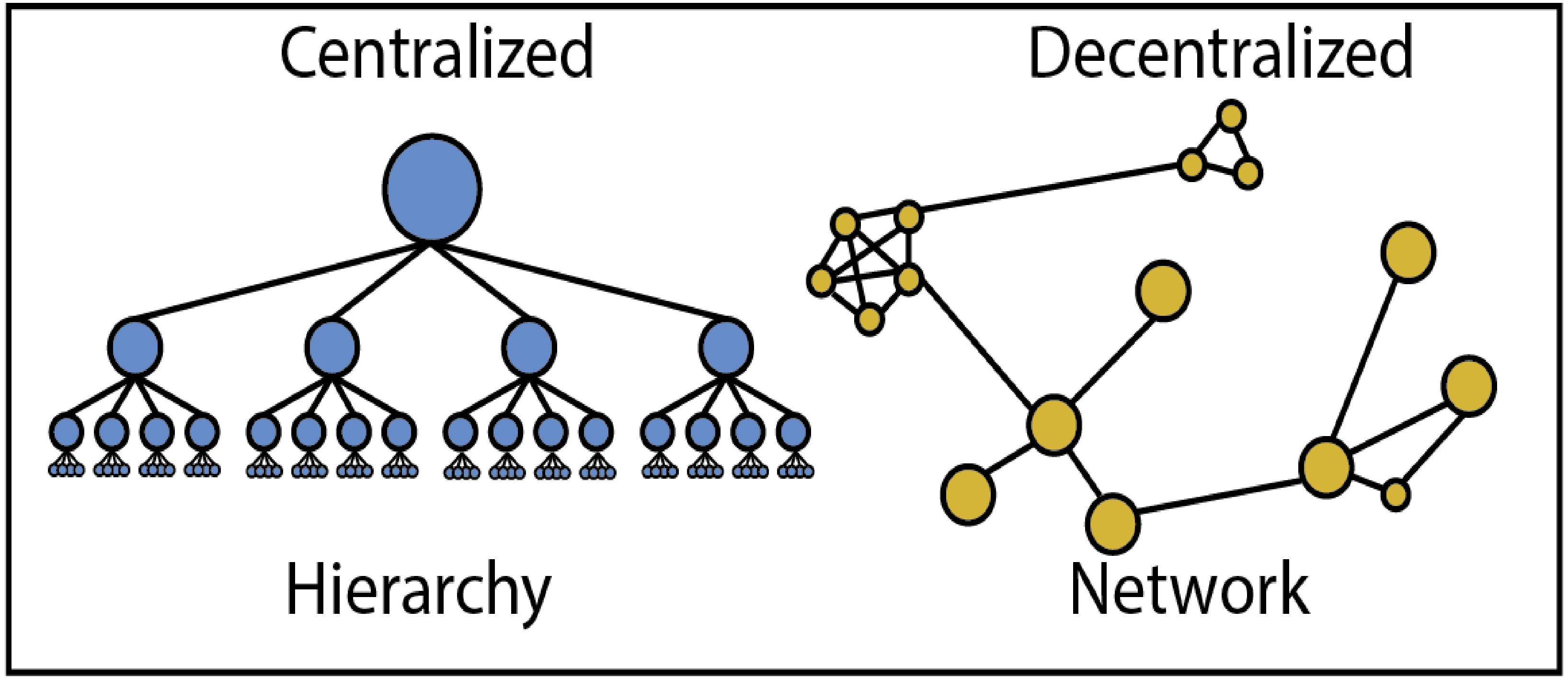
Shared Purpose
Actionable Knowledge
Common Consciousness

Risk Identification

Risk Prioritization

Actionable Risk Management

What are some of the Fusion models?



Fusion Center Outcomes

- Daily shared threat intelligence briefs
- Aggregated threat datasets and link data analysis
- IOC & Threat Actor hunting summaries
- Shared case management and statistics
- Research and Development (R&D)
- Quarterly senior leadership risk briefs

Fusion Center Guidelines

- Collaboratively develop and embrace a mission statement and identify goals for the fusion center.
- Create a governance structure
- Develop, publish and adhere to policies and procedures.
- Create a collaborative environment for the sharing of intelligence and information
- Leverage common systems, databases and networks to maximize sharing and handling of incidents and events.
- Create an environment of real-time seamless communication of information.
- Integrate people, process, systems and technology.
- Ensure people are properly trained.
- Identify redundancies and streamline operations.
- Focus on automation, data, AI
- Capture and demonstrate on-going ROI.

Next steps

- Seek senior leadership support.
- Start small
- Focus on Collaboration and Sharing of information
- Fuse data, tools, processes on few use cases.
- Communicate often.
- Celebrate successes and evaluate often.
- It is a multi-year approach.
- Key Goal “Turning Information and Intelligence Into Actionable Knowledge”