



ML/AI Exploration: Compliance Event Manager

Leslie A. McFarlin, Sr. UX Designer, EDP Value Stream



Introduction

Data security's ever-changing nature requires security measures to evolve quickly in ways that reduce the workload of security specialists, but ensure their judgments remain reliable.

Cognitive security systems are the latest evolutionary step, pairing self-learning systems with security specialists.

Cybersecurity Operations Centers could benefit greatly from a cognitive security solution due to their need to remain flexible, operate proactively, and respond quickly when security breaches occur.



Introduction

Per multiple market reports, analysts project CA to remain a key player in the cognitive security market until at least 2025.

By 2020, the worldwide market of ML- and AI-based security solutions will be \$10B.

Early adopters of AI-based products will see a boost in their profits that could translate to a 10% revenue gain for providers of those products.

Within the next 5 years, ML/AI will shift from focusing on algorithms to focusing on high-value data.



Introduction

CA possesses all of the major ingredients for developing a cognitive security solution across the Access Control, Enterprise Data Protection, and Mainframe Operations value streams.

Access Control provides raw data to supplement data collected via Enterprise Data Protection products.

Enterprise Data Protection products, especially CEM, offer a strong backbone upon which to construct a prediction and analytics that supports the bulk of cognitive security goals.

Mainframe Operations offers a model for surfacing intelligent system recommendations, and potentially providing feedback to such systems.




Introduction

Special thanks from the author goes out to the following Mainframe Security Team members:

Mitch Rozonkiewicz, Senior Principal Architect, for his assistance in identifying opportunities for bringing ML/AI to CEM, and understanding the features of security data collected by CEM.

Jim Broadhurst, CEM Product Owner, for his encouragement and support of the partnership between UX and engineering teams.



Cognitive Security Components

Understanding a Rising Trend

What Is Cognitive Security?

Structure of a Cognitive Security Solution

Benefits of Cognitive Security

Drawbacks of Cognitive Security



What Is Cognitive Security?

Cognitive security solutions rely upon the pairing of a human expert with an intelligent, self-learning system.

Self-learning systems use machine learning, natural language processing, and data mining to analyze large volumes of data to synthesize knowledge that supports continuous improvement.

Analyzing across a variety of data sources and interacting with human specialists ensures that cognitive security solutions operate as accurately as possible within a relevant context.



Structure of a Cognitive Security Solution

Perimeter Security

Awareness of an organization's security landscape, and the measures taken to secure access points, such as:

- Passwords
- Masking
- Encryption
- Access Permissions

Analysis & Prediction

Across security data from multiple sources, the system performs analyses to uncover trends it surfaces to human partners to support their decision-making and task completion.

Interactive Learning Layer

Understand unstructured data sources for a particular set of knowledge, reason through the contents of the data, and learn continuously via training from a human partner and from a constant stream of data.



Benefits of Cognitive Security

Proposes a human-machine partnership that offloads very simple and repetitive tasks, and very complex tasks, to a self-learning system to empower security specialists to perform other mission critical activities.

Enables a shift from reactivity to proactivity.

Analyzes data and synthesizes knowledge faster than a human.

Allows for a multi-dimensional view on security that enables analysis of subtle trends beyond the obvious ones due to anomalies, malicious insiders, and malware.



Drawbacks of Cognitive Security

As an analytical system reliant on data and human interaction to learn and become effective, these two points also stand as potential weaknesses for cognitive security.

Data quality affects the quality of the knowledge a cognitive system synthesizes, with lower quality requiring more training interactions to compensate.

During training interactions, users can transmit their own biases (due to a lack of knowledge, misunderstandings, or particular focus) to cognitive systems.



Supporting the Cybersecurity Operations Center

Pinpointing a Major User Group

Cybersecurity Operations Center Overview

CSOC Structure

CSOC Models

Supporting the CSOC



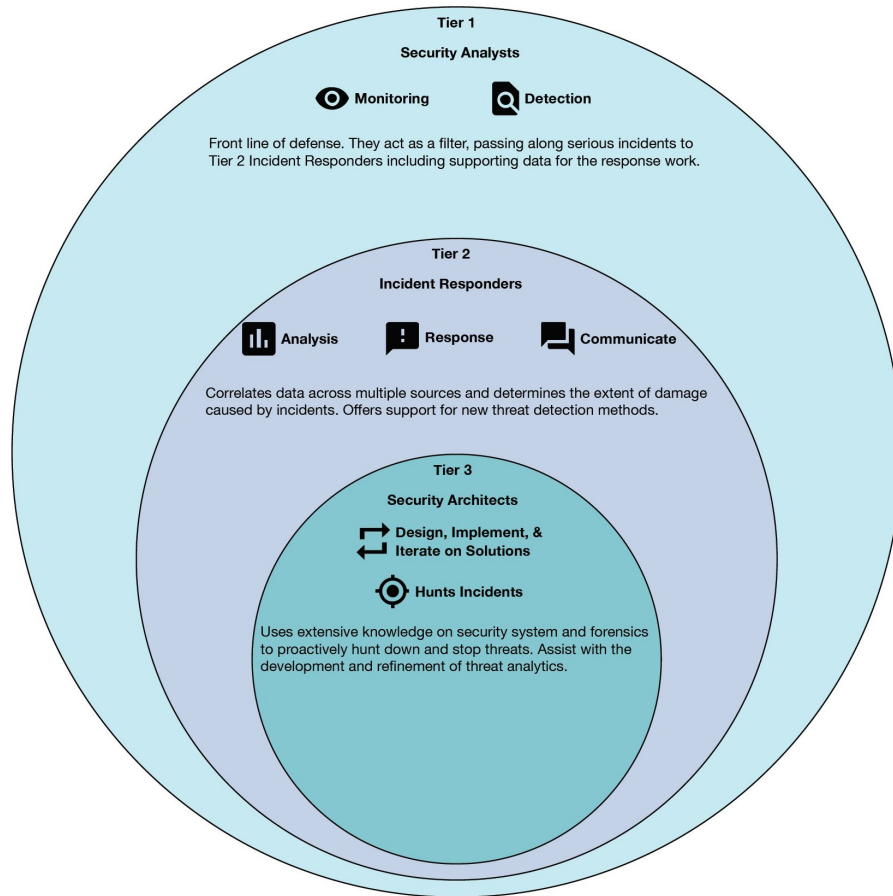
Cybersecurity Operations Center Overview

Cybersecurity Operations Center is a multi-tiered collection of security specialists who monitor a data environment's activities and seek to keep it secure, protected, and in compliance with regulations.

Blends people, process, and technology to enable a security strategy created in response to the ever-changing security landscape.

CSOC Structure

The CSOC organizes security specialists in a way that enables them to detect and neutralize threats as early as possible. As threats become more serious, they escalate to another tier to maximize response effectiveness.





CSOC Models

Fully Outsourced

Managed Security Service Provider (MSSP) fills all CSOC roles.

Communication to client is limited to:

- Incident Response.
- Queries about CSOC standards & procedures.

Hybrid: Internal+External Specialists

Model 1: 8x5 Business Hour Coverage

Employees fill CSOC roles during regular business hours.
MSSP fills all CSOC roles for non-business hours.

Model 2: Support In-House CSOC

Employees fill key CSOC roles.
MSSP fulfills roles dedicated to vigilance activities (monitoring & detecting).

Fully Internal

Model 1: 8x5 Business Hour Coverage

Employees fill CSOC roles during regular business hours.
Leverages technology to automate escalation and notifications per Security Architect recommendations.

Model 2: 24 x 7 Coverage

Employees fill CSOC roles on a schedule.
Automates features to reduce operations cost.



Supporting the CSOC

Processes and technologies used by a CSOC must keep its members operating flexibly and proactively.


Well-designed cognitive security solutions enable the goals of flexible and proactive operations by unburdening security specialists of time consuming tasks.

Regardless of the CSOC model an organization employs, cognitive security can provide benefits to each tier of a CSOC team.

CSOC teams are expensive, so technology must also balance cost with effectiveness and responsiveness.



Building a Cognitive Security Solution



Powering ML/AI with CEM

Evaluating the landscape for a CEM
+ ML/AI Strategy

Why Choose CEM for ML/AI?

Product Features

Industry Changes

Applying ML/AI to CEM



Why Choose CEM for ML/AI?

CEM has the potential to fit into a cognitive security strategy based upon product features and how they can be leveraged to support changes in :

- Core functionality

- Data collected

- Security team structure

- Security technology trends



Product Features: Core Functionality

CEM provides a valuable combination of data collection and descriptive data analysis:

Real-time data collection on security events from the policies set up in the application.

Reporting allows CEM users to combine multiple data points to describe compliance with policies.

Connections with SIEM applications enables more detailed analysis of security data points.



Product Features: Data Collected

Security is a data-rich domain, and between the ESM in use at an organization and CEM, a machine learning and AI-based solution would not face a shortage of training data.

ESMs feed data constantly to the SMF on z/OS that includes I/O activity, network activity, and errors.

Per engineering input, SMF data could be pulled for use via an utility.

CEM interacts with all 3 ESMs to capture security event data in real time.



Industry Changes: Security Team Structures

The security landscape changes constantly, requiring teams remain flexible and operate proactively to protect their organizations' data.

Cybersecurity Operations Center (CSOC) is a multi-tiered team structure that enables constant monitoring and detection and supports proactive measures and iterative security strategy refinement.

Depending upon an organization's resources, a CSOC may be fully staffed by an organization's employees, or have varying degrees of support from a managed security services provider.

Outsourcing of an organization's security monitoring services may indicate potential weaknesses in an organization's ability to handle or respond to security concerns.



Industry Changes: Need for Cognitive Security

Cognitive security combines different types of machine learning and AI to provide a self-learning system that interacts with security specialists to support the reliability of their judgments and appropriateness of their responses.



Applying ML/AI to CEM

Machine learning combines well with CEM's real-time data to provide a clear way to baseline security events and detect anomalies.

As pointed out by a CA architect from Team Woz, SMF contains a record of all security events on a mainframe, meaning baselines could be setup in a relatively short time.

Preprocessed data from CEM & CIA reports could also be analyzed via machine learning.

Report analysis could enable more effective proactive measures to security concerns, such as recommendations for policy changes or creation.



Cognitive Security & CEM

Cognitive security refers to continuously-learning systems that rely upon a combination of machine learning, natural language processing, data mining, and human interaction to develop hypotheses about what is happening on system.

It combines two concepts:

Deploying cognitive systems for the analysis of structured and unstructured security data to uncover insights and provide actionable recommendations for proactive security and business activities.

Supporting cognitive systems with technologies, techniques, people, and processes to provide relevant context for data and ensure accuracy of analyses and recommendations.



Assisting the Cybersecurity Operations Center



Research Activities

Creating Smarter Security
Solutions with Direct Insight

Data Literacy

Problem Definition

Idea Validation



Data Literacy

Data literacy refers to knowing what data are, and having an awareness of their collection, analysis, visualization, and use with respect to data security and data privacy (Crusoe, 2016).

Two personas to consider within the concept of data literacy:

Subjects, the people data is about, and who may have varying levels of data literacy.

Stewards, the people responsible for the security and privacy of collected data, and who may also have varying levels of data literacy.



Data Literacy

Within the context of CEM, the Steward persona will be of primary interest, as they are the end users who enact the policy on mainframe data.

Data is meaningless until it is analyzed, highlighting the importance of knowing what data are available, how it is being analyzed and presented, and how users intend to use it.

Data quality affects the analysis and presentation of the resulting output.



Data Literacy

Research on data literacy of CEM users should focus on the following topics:

What data does CEM collect?

What is the value of the collected CEM data?

What are the features of the CEM data that enable you to use it?



Problem Definition



Idea Validation



Thank You!

For questions or comments about this exploration document, please contact:

Leslie A. McFarlin, Senior UX Designer

leslie.mcfarlin@ca.com