Cybersecurity & Information Systems
Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Bridging Cybersecurity Gaps in Small Business Security Operation Centers (SOCs) Using Artificial Intelligence (AI)-Enabled Tools

Report Number:

CSIAC-BCO-2024-612

Completed June 2024

CSIAC is a U.S. Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Olutoye Sekiteri
Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense of any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
13-06-2024

2. REPORT TYPE
Technical Research Report

3. DATES COVERED *(From – To)*

4. TITLE AND SUBTITLE

Bridging Cybersecurity Gaps in Small Business Security Operation Centers (SOCs)
Using Artificial Intelligence (AI)-Enabled Tools

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)

Olutoye Sekiteri

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Cybersecurity & Information Systems Information Analysis Center (CSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

CSIAC-BCO-2024-612

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was tasked with researching cybertools and technologies to differentiate between various cyberevents and behaviors. CSIAC identified common cybersecurity shortcomings of small businesses, with the correlation between the size of an organization and its access to viable cybertools, technologies, and intelligence. CSIAC also identified how artificial intelligence (AI)-driven behavioral analytics can assist in enabling security operation center (SOC) analysts and cybersecurity professionals with protecting their threat environment and making informed decisions. CSIAC identified cybertools and software commonly used in SOCs, their known limitations, and Cybersecurity & Infrastructure Security Agency use cases of AI cybersecurity solutions. The cyberlandscape is always changing with the constant addition of new software, hardware, vulnerabilities, cyberthreats, and malware. As cyberadversaries continue to innovate new, more sophisticated malware and intrusion methods, small organizations increasingly rely on information technology products and services to run operations and store, transmit, and process data. With the U.S. Department of Defense's efforts to bring more small businesses into the defense industry and its emphasis on eliminating cybersecurity gaps and protecting government information systems, small businesses will need viable, practical, and actionable cybersecurity guidance, solutions, and intelligence that enable them to cost effectively address cybersecurity risks.

15. SUBJECT TERMS
small business, cybersecurity, artificial intelligence, machine learning, behavioral analytics, cybertools

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ted Welsh, CSIAC Director
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	36	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

About

DTIC and CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (DoDIAC), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoDIAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

TI Research

A chief service of the DoDIAC is free technical inquiry (TI) research limited to four research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. Given the limited duration of the research effort, this report is not intended to be a deep, comprehensive analysis but rather a curated compilation of relevant information to give the reader/inquirer a "head start" or direction for continued research.

Abstract

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was tasked with researching cybertools and technologies to differentiate between various cyberevents and behaviors. CSIAC identified common cybersecurity shortcomings of small businesses, with the correlation between the size of an organization and its access to viable cybertools, technologies, and intelligence. CSIAC also identified how artificial intelligence (AI)-driven behavioral analytics can assist in enabling security operation center (SOC) analysts and cybersecurity professionals with protecting their threat environment and making informed decisions. CSIAC identified cybertools and software commonly used in SOCs, their known limitations, and Cybersecurity & Infrastructure Security Agency use cases of AI cybersecurity solutions. The cyberlandscape is always changing with the constant addition of new software, hardware, vulnerabilities, cyberthreats, and malware. As cyberadversaries continue to innovate new, more sophisticated malware and intrusion methods, small organizations increasingly rely on information technology products and services to run operations and store, transmit, and process data. With the U.S. Department of Defense's efforts to bring more small businesses into the defense industry and its emphasis on eliminating cybersecurity gaps and protecting government information systems, small businesses will need viable, practical, and actionable cybersecurity guidance, solutions, and intelligence that enable them to cost effectively address cybersecurity risks.

Contents

List of Figures

1.0 TI Request

1.1 Inquiry

How are cybertools and cybertechnologies used in differentiating between automated reconnaissance and enumeration events, as well as hands-on-keyboard events?

1.2 Description

The Cybersecurity and Information Systems Information Analysis Center was asked to provide information on cybertools and technologies that can distinguish between different cyberevents. The inquirer noted the existence of shortcomings in the cybersecurity and threat hunting capabilities specifically for small organizations and wanted examples of how to bridge the gap in capabilities using artificial intelligence (AI)/machine learning (ML) software solutions and platforms.

2.0 TI Response

2.1 Challenges Small Businesses Face in Security Operation Centers (SOCs)

What is a small business? The U.S. Small Business Administration (SBA) "defines a small business by firm revenue (ranging from $1 million to over $40 million) and employment (from 100 to over 1,500 employees). For example, according to the SBA definition, a roofing contractor is defined as a small business if it has annual revenues of $16.5 million or less" [1]. Small businesses are the pillars of foundation for the U.S economy and make up most of the businesses in the United States. In fact, the SBA reveals that "33.3 million businesses in the United States qualify as small businesses, making up 99.9% of all U.S. businesses" [2]. "Small businesses employ 61.7 million Americans, totaling 46.4% of private-sector employees" [3]. These numbers not only reflect the dominance of small enterprises in the business sector but also show their significant role in generating employment and contributing to economic stability. Even though small businesses make up the majority of the U.S. economy, they are more likely to not be properly prepared or lack the ideal setup to be ready to respond to a cyberevent. Small businesses tend to lack the personnel, budget, cybersecurity training, and threat intelligence to react to a cyberattack or incident efficiently and effectively. These factors are also the main reasons why cyberadversaries view small businesses as easy targets; they are the least prepared to fend for themselves in the cyber-realm.

2.1.1 Lack of Personnel

As the name of this section implies, small businesses do not have a huge number of employees. Therefore, in wake of a major cyberevent, small businesses are at a disadvantage in having the right hands on deck to respond correctly at scale. The Western Telecommunications Alliance (WTA) is [4]:

> …a national trade association comprising more than 250 rural broadband telecommunications carriers [and has provided] its comments on the Preliminary Cybersecurity Framework proposed by the National Institute of Standards and Technology (NIST).
>
> WTA's members and other small rural companies have little hope of being able to hire or retain experienced cybersecurity professionals and generally lack the resources to allow their small technical and administrative staffs to devote more than a couple hours per week to cybersecurity activities. For example, a small carrier with [two to five] somewhat cyberknowledgeable managers and technicians will drop everything to react to a cyberattack or tangible threat but does not have the staff resources to engage in extensive cybersecurity meetings, planning and training.

This highlights a common problem that small businesses have when developing an initial cybersecurity plan and delegating responsibilities to their limited number of employees. According to small business statistics, "only 14% of small businesses have a dedicated cybersecurity team [and] 22% of small businesses do not have any type of cybersecurity plan in place" [5].

2.1.2 Cybersecurity Is Not Prioritized

The smallest of small businesses is the least concerned about cyberattacks. On CNBC's SurveyMonkey Small Business Index Q2 2022 Survey [6], which surveyed 2,027 small businesses, only 5% of businesses expressed cybersecurity to be the biggest risk to their business. In Hiscox's annual Cyber Readiness Report [7], only about 33% of U.S. small businesses consider cyber-risk high or very high. In addition, 61% of businesses surveyed expressed no concern that they would be the victim of a cyberattack within the next year. Few small business owners rate cyberthreats as their top business risk, and fewer than half consider it to be a concern. Nevertheless, a majority expresses confidence in the ability to respond to a cyberattack. According to the survey, 62% of the businesses stated they were confident in their ability to respond quickly to a cyberevent [6]. To cover for information system, computer, or technology-related losses associated after a cyberevent, 53% of small businesses have opted to use standalone cyber-risk insurance, cyberliability insurance, or cybercoverage through another policy to protect themselves [7].

2.1.3 Budget Constraints and Lack of Cybertraining and Intelligence

According to an UpCity article and survey [8], 68% of small businesses paid anywhere between $0–$1,999 on cybersecurity per month pre-COVID. That number jumped to 72% in 2022. "Despite a 10% increase in median [information technology] IT budgets and a 24% increase in cybersecurity spending over the next 12 months, 59% of small businesses did not use security-awareness training. Further, 43% of the businesses surveyed did not have network-based firewalls" and 41% did not use data-backup recovery and restoration systems [7]. Budget constraints on small businesses make it hard to hire dedicated cyberstaff to manage and maintain their threat environment. This lack of funds also creates an issue with having the proper equipment and software at hand to respond to cyberincidents. For the personnel that a small business may have on hand to respond, a lack of cybertraining leaves employees unprepared for social-engineering attempts, malware execution attempts, and common human error that is experienced.

Along with the lack of training and proper systems to protect a small organization, small businesses may feel overwhelmed by the huge amount of information out there on potential vulnerabilities, threats, and solutions. Without the proper training or intelligence to know where to look for known and emerging threats, small organizations are at a big disadvantage. Some cyberthreat intelligence platforms are even "for pay" or paired with existing threat detection and response software that need to be purchased. This overload of information may make it hard for small businesses to know exactly where to start with cybersecurity and can prevent an organization from acting at all and, rather, accepting all the risk. Having a lack of skilled professionals and proper cybertools makes it difficult to maintain an organization's cybersecurity posture, strategy, and policies. This lack of resources creates gaps in knowledge, experience, and cyber-response capabilities, making organizations less prepared to address a cyberincident. According to small business statistics, "the average cost of a cyberattack on a small business is $200,000 [and about] 60% of small businesses that suffer a cyberattack go out of business within 6 months" [5]. Improving cybersecurity for most organizations is not seen as a profitable endeavor, and they will try to reduce cybersecurity risk as much as possible with the least capital.

2.1.4 Data Overload

The overall cybersecurity landscape has changed drastically within the past decade. One major driver of this change is the increase in the amount and size of the data being processed. "The amount of data generated annually has grown year over year since 2010. It is estimated that 90% of the world's data was generated in the last two years alone" [9]. Additionally, every two years, the volume of data across the world doubles in size. "In the space of 13 years, this figure has increased by an estimated 74× from just 2 zettabytes [ZB] in 2010. The 120 ZB generated in 2023 are expected to increase by over 150% in 2025, hitting 181 ZB" [9].

Many of today's IT environments are hybrid or multicloud to handle the constant influx of raw data and new intelligence the organization's hardware, software, and applications may output. Cybersecurity teams often have to leverage and switch between various cybertools to sift through stored data streams and complete tasks such as troubleshooting, threat hunting, and vulnerability assessments. This reliance on multiple IT management, monitoring, and response tools to complete the same or similar tasks is known as tool sprawl. This overuse of multiple tools can create an overwhelming sea of IT alerts and metrics. Too much IT and log data create a challenge of analyzing and pinpointing specific issues, reducing response times, and limiting troubleshooting accuracy. This can complicate things and make it hard for a cyberprofessional to make sense of the data and correlate them to the underlying cyberissues.

2.1.5 Small Organizations Are Seen as "Easy Targets"

According to Verizon's "2024 Data Breach Investigations Report" [10]: "14% of breaches involved the exploitation of vulnerabilities as an initial access step [and] 15% of breaches involved a third-party or supplier, such as software supply chains, hosting partner infrastructures, or data custodians. [Further,] 68% of breaches involved a nonmalicious human element, like a person falling victim to a phishing attempt or making an error." Roughly one third of all breaches involved ransomware or some other extortion technique.

Cyberadversaries are aware of the shortcoming of small businesses in the cyber-realm. There is a common perception that small businesses are easier targets due to the belief that they have weaker defenses and are not as likely to have robust cybersecurity capabilities. Small businesses may not have the financial power of larger corporations, but they still have enough monetary value and relevance to motivate hackers. A small business may also be in partnership with larger organizations in its supply chain. Attackers can gain an understanding of the interconnectedness of business operations and target a small business within a supply chain to get access to the larger organizations' systems and data. This type of calculated targeting can expose customer data, payment information, intellectual property, and trade secrets. In the case of the U.S. Department of Defense (DoD), government/military information systems can be at risk, as well as controlled unclassified information (CUI) and classified documents.

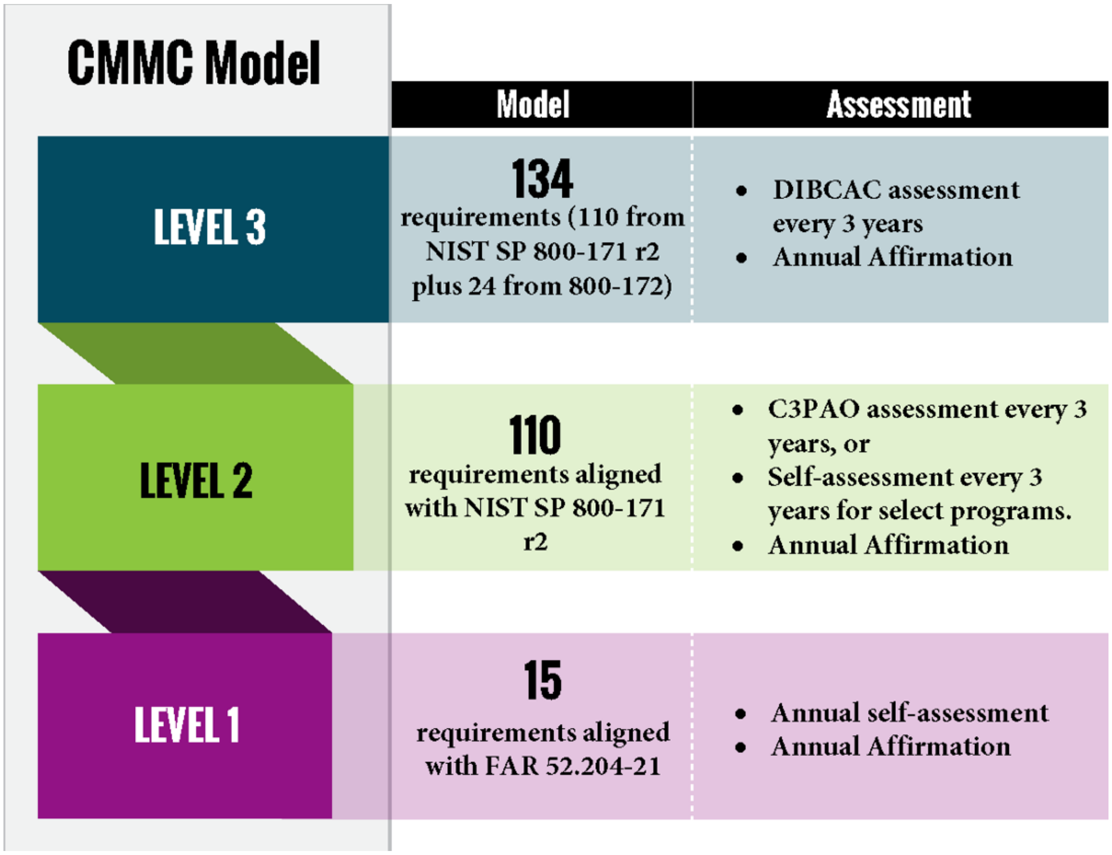
An example of this concept at play can be seen firsthand with the July 2024 leak of documents stolen from Pentagon contactor, Leidos [11].

> Hackers…breached the systems of Leidos Holdings, a major contractor for the U.S. government, and leaked stolen internal documents online. The leak is believed to be tied to a previously disclosed breach of a Diligent Corp system that Leidos used [to host information for internal investigations.]
>
> A spokesperson from Diligent stated that the leak appears to have stemmed from a 2022 hack affecting its subsidiary Steele Compliance Solutions, acquired in 2021.
>
> The breach of Diligent in 2022 reportedly involved two separate incidents, which have now led to the exposure of sensitive documents from Leidos.

A hack of a company's subsidiary in 2021 eventually led to the breach of a larger organization's sensitive data three years later. This situation highlights the current challenges and risks faced by major IT service providers in protecting critical information [11].

2.1.6 Need for Compliant Systems and Applications

For small businesses to be awarded new contracts with the DoD, organizations should be aiming to be Defense Federal Acquisition Regulation Supplement (DFARS) and Cybersecurity Maturity Model Certification (CMMC) compliant. DFARS outlines a common set of cybersecurity regulations that defense contractors and suppliers must follow, such as intrusion monitoring, cyberincident reporting, proper handling of CUI information, ensuring subcontractor compliance, and meeting requirements outlined in NIST Special Publication (SP) 800-171 [12]. The CMMC program is based on DFARS 252.204-7012 [13], builds on its concepts to add a verification component, seeks to verify the cybersecurity of defense contractors relative to NIST SP 800 171 [12], and further strengthens the defense industrial base. The CMMC program ensures that private-sector companies doing work for the DoD as part of the defense industrial base demonstrate that their computer networks and cybersecurity practices are up to the task of defending against intrusions by adversaries who may want access to sensitive unclassified information, CUI, and data about federal government contracts and weapons systems development. CMMC assessments will be available as early as quarter (Q)1 2025, and a phased rollout of CMMC as a contractual requirement is estimated to begin around Q3 of 2025. CMMC has recently been simplified from five to three maturity levels (Figure 1).



CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

Note: DIBCAC = Defense Industrial Base Cybersecurity Assessment Center, C3PAO = CMMC Third-Party Assessment Organization. NIST SP 800 171 [12], NIST SP 800-172 [14], Federal Acquisition Regulation (FAR) 52.204-21 [15].

Figure 1. CMMC Model [16].

An article by Lopez details the three levels, as described by the director of the CMMC program management office [17]:

> Level one compliance asks contractors to self-assess their ability to provide basic protection of federal contract information. At level two, which deals with general protection of [CUI], companies will either self-assess or seek assessment by a CMMC third-party assessment organization, depending on the nature of the information they will be expected to process.

> For level three, the highest level, compliance requires companies to demonstrate an ability to protect higher levels of [CUI]. Certification at this level must be completed with an assessment by [the] DoD's own Defense Industrial Base Cybersecurity Assessment Center.
>
> The CMMC has also been simplified in other ways to make it easier for private companies to demonstrate cybersecurity compliance and become eligible to contribute to national security.

Although CMMC's maturity levels have been simplified, "it typically takes organizations anywhere from 6 to 18 months to prepare [for a CMMC] assessment" [18]. This can take even longer if any issues arise along the way. Small businesses may find CMMC compliance to be an expensive task and may not be able to recoup losses. Given the technical expertise required to make necessary cybersecurity changes, small organizations may also find obtaining CMMC certification to be too complex a task to handle on their own.

Regarding cloud applications used by small businesses within the DoD, they must be authorized by the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP was established "in 2011 to provide a cost-effective, risk-based approach for the adoption of secure cloud services…across the federal government by providing a standardized approach to security and risk assessment" for cloud technologies and federal agencies [19]. According to FedRAMP, compliance is required for all cloud-service providers that offer services to federal agencies and all federal agencies that transmit sensitive data over the cloud. FedRAMP maintains a searchable and sortable "marketplace" for authorized cloud software that has achieved FedRAMP designation, making it easier to find cloud software. FedRAMP helps eliminate redundant and inconsistent efforts, supports the adoption of cloud computing and innovative technologies, and promotes the use of properly secured systems and applications. Small businesses can potentially find themselves limited by the selection of FedRAMP-authorized software and may need to make adjustments to their current IT environment to integrate specific applications. These adjustments can be costly and take significant time to implement. Resources required for small businesses seeking to obtain FedRAMP authority to operate can pose a huge barrier. This can cause a business to continue using unauthorized software to maintain operations.

2.2 AI-Driven Analytics

This section describes types of AI analytics, behavioral analytics, how AI-driven behavioral analytics works, and what benefits they provide.

2.2.1 Types of AI Analytics

Four types of AI analytics are [20]:

1. Descriptive Analytics: AI is used to sift through large amounts of structured and unstructured data to identify patterns, trends, and correlations to provide an accurate and comprehensive understanding of past performance.
2. Diagnostic Analytics: AI analyzes complex datasets to correlate information and understand the root cause of an event or issue.
3. Predictive Analytics: AI uses advanced algorithms to examine historical data and identify patterns, supporting more accurate predictions for future trends and outcomes.
4. Prescriptive Analytics: AI analyzes datasets and provides actionable recommendations, suggesting a best course of action for different scenarios to aid decision-makers.

2.2.2 Behavioral Analytics

Behavioral analysis within an SOC involves observing a threat environment's activity within its systems; trying to decern between normal, acceptable behaviors and anomalous activity; and identifying potential threats. A traditional intrusion detection system (IDS)/intrusion prevention system (IPS) will use a predefined rule-based or signature-based system of detection for potential threats. This method has worked well for threats that are known and have a good amount of cyberthreat intelligence surrounding them, but they fail to meet the needs required to detect new, previously unseen cyberattacks, malware, and zero-day exploits. Adversaries are always evolving and finding new ways to infiltrate internal networks and remain hidden. Waiting to find a formally recorded cyberincident or example of malware in use just to combat against it is not ideal and can leave an organization two steps behind threat actors [21].

2.2.3 How Does AI-Driven Behavioral Analytics Work?

Using AI for behavioral analytics can touch many of the same concepts as the previously listed types of AI analytics. AI-enabled behavioral analytics starts by collecting data from current technology stacks and systems during normal hours of operation. These data include user activities, system logs, and network traffic. This is done to establish the foundation and baseline for what is considered normal in an organization's engagement, devices, applications, files, and network. An AI algorithm will use these collected data to train itself on what organizational behaviors in the system it observed to be normal. The more diverse, robust, and comprehensive the collected data are, the more accurate the algorithm can distinguish behaviors from normal and abnormal. The trained AI system that is deployed will continuously and actively monitor system activities to identify behaviors and patterns. If the AI algorithm discovers a pattern of behavior that deviates from the baseline norm established in training, then it flags the unusual behavior as an instance of a potential security threat. These anomalies can range from large-scale security breaches to minor policy violations. At this point, a human within the loop will review the cyberevent to ensure that the AI algorithm has flagged the anomalous behavior accurately and will then quickly try to correct flag issues if need be. This process of review for the AI algorithm's output also provides an opportunity to reinforce and improve the AI algorithm over time, through minor adjustments [21]. Figure 2 depicts an AI correlation map to support network detection.

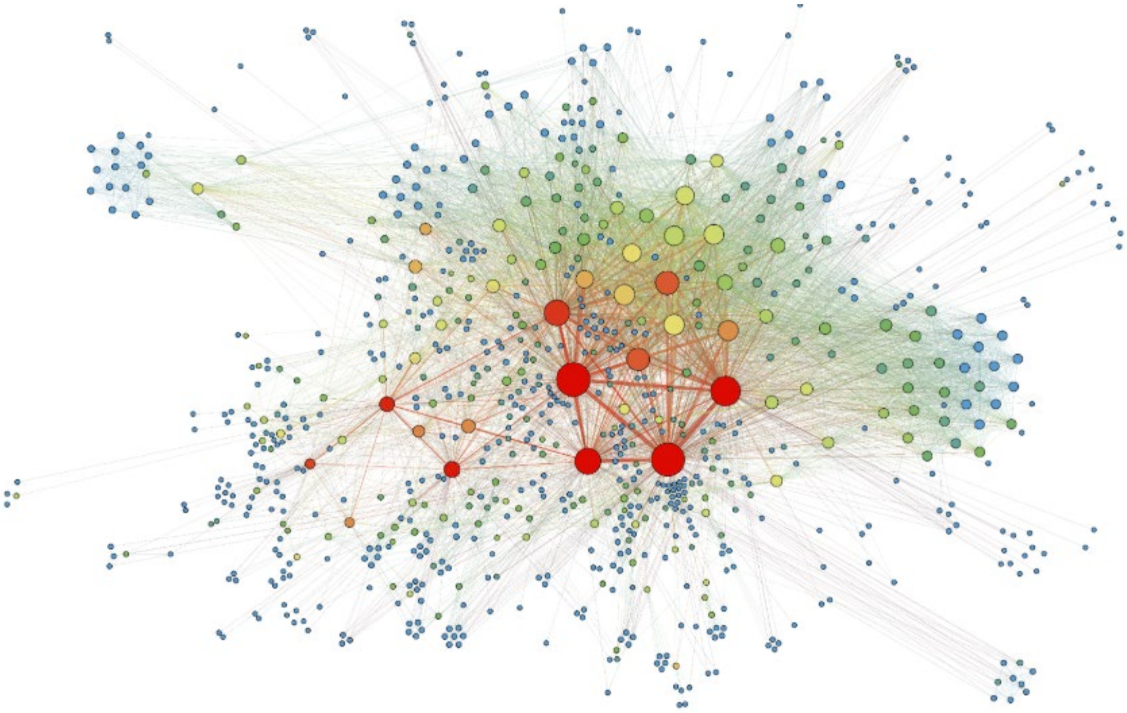


Figure 2. AI Correlation Network Map From dMetrics's Platform to Support Threat Network Detection [22].

2.2.4 What Benefits Do AI-Driven Behavioral Analytics Provide?

Some benefits of AI-driven behavioral analytics are [21]:

- Ability to Handle Large Volumes of Data at Scale: These systems have the capacity to process and analyze huge datasets quickly. They can also scale up to larger networks while maintaining threat-detection capabilities.
- General Holistic View: These systems have the ability to analyze patterns of behaviors across an organization's complete attack surface, providing a line-of-threat defense that is not limited by attack methods used by adversaries or specific tools. The

generalization of behavioral patterns provides an adaptable defense against a wide spectrum of cyberattacks, including unseen and zero-day threats.

- Real-Time Threat Detection and Quick Response Times: AI-driven behavioral analysis systems detect anomalies as they happen, allowing an instantaneous response to threats and minimizing the effects they may have caused.
- Predictive Capabilities: By training on previous behaviors, cyberevents, and trends, AI-driven algorithms are able to anticipate potential threats in the future, moving away from relying solely on static libraries or policies and allowing for preemptive measures to reduce risk.
- Ability to Reduce False Positives: With ongoing training, retraining, and human intervention via corrections, these AI algorithms improve their ability to differentiate between anomalous activity and a benign deviation from the norm. This reduces the resources and time spent sifting through and investigating false positives.
- Cloud Utilization: AI-driven behavioral analysis can leverage cloud resources for use of viable, up-to-date cyberthreat intelligence and to conduct large-scale analysis alongside a huge set of variables and data.

2.3 Common Cybertools Used in SOCs and Potential AI Solutions

This section discusses common cybertools used in SOCs, AI-driven cybersecurity concepts, and DoD and government use cases for cybersecurity.

2.3.1 Common Cybertools Used in SOCs

The following details common cybertools used in SOCs, along with their limitations and the benefits AI-enabled solutions can provide.

- IDS: “A network security tool that monitors network traffic for known malicious activity, suspicious activity, or security policy violations” [23].
    - Limitations
        - Can require ample resources to implement, such as network bandwidth, storage capacity, maintenance, and capital.
        - Is only meant to detect activity and violations and is not designed to act on those events.
        - Needs experienced human engineer to analyze and act on data.
        - Relies on malware signature libraries that need to be constantly updated.

    - Can have data overload.
    - Can have false positives.

  - Benefits AI-Enabled Solutions Can Provide

    - Uses behavioral analytics and AI algorithms to detect deviations in baseline operations.
    - Identifies known and unknown threats, eliminating the reliance on only signature libraries.
    - Is highly scalable to handle large amounts of data to reduce overload.
    - Reduces false positives with intelligent analysis, correlation and contextual understanding of network environment and behavior.

- IPS: A network security tool that monitors network traffic for potential threats, blocks threats through an automated process, alerts the security team, and eliminates risky connections [24].

  - Limitations

    - Can require ample resources to implement, such as network bandwidth, storage capacity, maintenance, and capital.
    - Relies on malware signature libraries that need to be constantly updated.
    - Relies on a set of predefined security policies, controls, and rulesets that must be configured correctly and fine-tuned.
    - Can have data overload.
    - Can have false positives.

  - Benefits AI-Enabled Solutions Can Provide

    - Uses behavioral analysis and AI algorithms to detect deviations in baseline operations.
    - Identifies known and unknown threats, eliminating the reliance on only signature libraries.
    - Allows IPS to dynamically make changes to mitigate intrusions, eliminating the reliance on predefined security policies and rulesets.
    - Is highly scalable to handle large amounts of data to reduce overload.
    - Reduces false positives with intelligent analysis, correlation, and contextual understanding of network environment and behavior.

- Firewall: A network security tool that filters, monitors, and blocks network traffic passing between network gateways based on a set of predefined security policies/rules an organization creates [25].
  - Limitations
    - Relies on a set of predefined security policies, controls, and rulesets that must be configured correctly and fine-tuned.
    - Can protect against known cyberthreats but will not be able to respond to complex cyberattacks and threats like zero-day exploits.
    - Cannot stop internal users from accessing data or information from malicious websites, making them vulnerable to internal threats or attacks.
  - Benefits AI-Enabled Solutions Can Provide
    - Allows firewall to dynamically make changes to mitigate network intrusions, eliminating the reliance on predefined security policies and rulesets.
    - Uses behavioral analytics and AI algorithms to detect deviations in baseline operations and identify complex cyberattacks and threats like zero-day exploits.
- Network Detection and Response (NDR): A network security technology that continuously monitors network traffic from physical and cloud-based environments to enable security teams to detect abnormal system behaviors by applying behavioral analytics to network traffic data. It detects adversary activity, responds to incidents, and improves organization security posture [26].
  - Limitations
    - Can require ample resources to implement, such as network bandwidth, storage capacity, maintenance, and capital.
    - Has lack of scope. NDR is a standalone solution that only monitors network traffic and cannot view events that happen on endpoints, such a registry change on a workstation.
    - Cannot respond to complex multidomain cyberattacks and threats.
    - Can have data overload.
    - Can have false positives.

  - Benefits AI-Enabled Solutions Can Provide
    - Is highly scalable to handle large amounts of data to reduce overload.
    - Reduces false positives with intelligent analysis, correlation, and contextual understanding of network environment and behaviors.

- Endpoint Detection and Response (EDR): An endpoint security tool that continuously monitors end-user devices to detect and respond to potential cyberthreats [27].
  - Limitations
    - Has lack of scope. EDR is a standalone solution that only focuses on endpoint logs for devices and has limited network scope.
    - Cannot respond to complex multidomain cyberattacks and threats.
    - Relies on malware signature library that needs to be constantly updated.
    - Can send alerts automatically, but some events may still require a manual review of endpoint data or intervention for incident response to prevent cyberattacks.
    - Can have data overload.
    - Can have false positives.
  - Benefits AI-Enabled Solutions Can Provide
    - Identifies known and unknown threats, eliminating the reliance on only signature libraries.
    - Is highly scalable to handle large amounts of data to reduce overload.
    - Reduces false positives with intelligent analysis, correlation, and contextual understanding of endpoint landscape and behaviors.

- Extended Detection and Response (XDR): A unified security incident platform that collects threat data from multiple data streams, including endpoint data, network data, and cloud data within an organization technology stack. XDR leverages data correlation across various sources to detect complex and coordinated attacks and also offers automated response actions, enabling rapid containment and mitigation of threats [28].
  - Limitations
    - Is a complex mutidomain solution that requires ample capital, resources, expertise, and a careful implementation planning process.

- Can have data overload.
- Can create false positives for the diverse types of data being correlated.

- Benefits AI-Enabled Solutions Can Provide
  - Is highly scalable and able to handle large amounts of data of diverse data types.
  - Reduces false positives with intelligent analysis, correlation, and contextual understanding of unified security environments and behaviors.

- Security Information and Event Management (SIEM): A cybersecurity solution that helps organizations collect, analyze, and correlate log data and security event data from various sources within an IT infrastructure. SIEM systems provide real-time monitoring, threat detection, incident response, and compliance management capabilities [29].
  - Limitations
    - Has lack of scope. SIEMs are standalone systems that focus on various log data and provide limited endpoint visibility.
    - Requires a large cost and ample resources for implementation, maintenance, and ongoing use of system.
    - Primarily relies on rule-based correlation that needs to constantly be updated and fine-tuned manually.
    - Can have data overload. The large amount of log data can bring about many alerts.
    - Can have false positives.
  - Benefits AI-Enabled Solutions Can Provide
    - Can dynamically correlate events and assets, eliminating the reliance on predefined rule-based correlation.
    - Is highly scalable and able to handle large amounts of log data.
    - Reduces false positives with intelligent analysis, correlation, and contextual understanding of unified security environments.

- Security Orchestration, Automation, and Response: A security tool “that enables security teams to integrate and coordinate between separate security tools, automate repetitive tasks, and streamline incident and threat response workflows” [30].

- Limitations
    - Cannot address organizations poor cybersecurity structure, policies, and culture.
    - Must send automated workflows correctly and implement them carefully.
- Benefits AI-Enabled Solutions Can Provide
    - Can carry out automated workflows with less human intervention in between.
    - Has workflows and can be easily tested for efficiency.

- Managed Detection and Response (MDR): An outsourced cybersecurity service that combines advanced technology and human expertise to provide endpoint, network, and cloud environment monitoring 24/7, as well as threat detection and response [31].
    - Limitations
        - Still requires an outsourced MDR team to have context and knowledge of the internal IT environment.
        - May not support current technology stack and may therefore have a need for replacement of applications to integrate. MDRs normally do not allow for custom thread feed integration [32].
        - Has limited visibility into the extent of the MDR investigation.
        - Has possibility that the security operation metrics used to convey information may not be ideal for the insight the organization wants to gain.
        - Relies on third party for a good chunk of cyberoperations.
    - Benefits AI-Enabled Solutions Can Provide
        - Provides MDR teams with the ability to leverage AI/ML capabilities and benefits to aid in providing third-party services.
        - Identifies known and unknown threats, eliminating the reliance on only signature libraries.
        - Is highly scalable to handle large amounts of data to reduce overload.
        - Reduces false positives with intelligent analysis, correlation, and contextual understanding of endpoint landscape and behaviors.
- Threat Intelligence Platforms: An informational tool that provides security teams with intel on known malware and other threats giving accurate and efficient threat identification, investigation, and response capabilities. Allows cyberprofessionals to

spend more time analyzing data and investigating potential threats, instead of developing their own threat knowledge base. Threat intelligence platforms also enable security and threat intelligence teams to easily share threat intelligence data with relevant stakeholders, security systems, and the greater cybercommunity [33].

- Limitations
    - With the ever-changing diversity of the cyberthreat landscape, security teams are forced to process larger sets of data through more security tools.
    - To make informed decisions, these platforms need an understanding of the full context surrounding a threat that includes historical data, relationships among data objects, data about the adversary, and background on how the threat has been used in the past [34].
    - Can be challenging for less experienced cyberprofessionals to make sense of the threat data.
- Benefits AI-Enabled Solutions Can Provide
    - Allows for easy sharing of threat information between organizations over the cloud.
    - Can integrate threat intelligence feeds into the cybersolutions to aid in correlation, threat detection, and intrusion mitigation.

- Vulnerability Scanners: An automated tool that can scan an organization's network, specific devices, or web applications for weaknesses in its environment. Can also provide insight into the risk associated with each vulnerability and recommendations on how to mitigate that vulnerability [35].
    - Limitations
        - Often operates on predefined checks, policies, and controls, so the scanner is only as good as the rules coded into it.
        - Can lack depth in understanding the more intricate aspects of an IT environment, applications, and nuanced business logic.
        - Can have false positives.

- Benefits AI-Enabled Solutions Can Provide
  - Allows vulnerability scanners to dynamically scan for vulnerabilities, factor in new threat intelligence, and eliminate the reliance on predefined security policies and rulesets.
  - Allows scanner to better correlate and understand IT environments.
  - Reduces false positives with intelligent analysis, correlation, and contextual understanding of unified security environments and behaviors.

Figure 3. An Air Force Captain Cyberoperator Assigned to the 276th Cyber Operations Squadron, Maryland Air National Guard, Works on Computer at Home After Participating in the Cybershield Exercise [36].

2.3.2 AI-Driven Cybersecurity Concepts

AI and ML are huge disruptors throughout many industries and are core components of many next-generation cybersecurity tools used within SOCs. Due to AI's distinctive capacity to process and analyze large amounts of data, differentiate behaviors, correlate events and dependencies, and generate predictive insights in a short period of time, AI-based analytics and cybersecurity have been applied across a wide range of tools and use cases.

In most AI-powered IPSs, SIEMs, and XDRs, regular end-to-end processes are automated and conducted autonomously, significantly reducing the workload of security analysts and enabling them to strategize and focus more on mitigating threats. AI can improve the accuracy and response time in these tools, as it automatically identifies threat patterns and deviations from baseline operations, in return reducing alert fatigue in security staff and decreasing security risks and false positives. As organizations increasingly move their IT operations to the cloud, cloud-native, next-generation, cybersecurity applications are giving organizations the scalability and flexibility they need to expand their security capabilities as they evolve. For example, the deployment and maintenance of traditional on-premises SIEMs can take up significant time and resources, making it unrealistic for smaller companies to handle. Cloud-based SIEMs do not present less of those hurdles, as they have a quicker onboarding process and require less upkeep. Cloud-based delivery SIEMs enable all users and devices within a network to be managed from a single dashboard, providing convenience and ease of use. The implementation of cloud-based cybersecurity applications opens the door for the integration of cyberthreat intelligence feeds within SIEMs. This enables organizations to monitor and compare their internal data with information and insights contained in threat feeds. It also ensures that organizations are well equipped by having a good grasp of the threat landscape as it evolves, in real time.

Traditional vulnerability scanners use a set of predefined signatures, patterns, and rules to assess vulnerabilities. This software, while still valuable, is not able to keep up with the changing landscape of cyberthreats and relies on predefined checks, policies, and controls. AI-powered vulnerability scanners use ML algorithms to train on huge amounts of up-to-date cyberthreat intelligence data to help identify potential vulnerabilities proactively, not reactively [37]. The continuous training from ML allows the scanner to pick up on vulnerabilities that would go under the radar for a traditional scanner. AI-driven vulnerability scanners adapt to environments dynamically and detect activities that stray away from expected behaviors, empowering SOC teams to discover vulnerabilities before they can be exploited and be a step ahead of emerging threats and risks. AI-powered vulnerability scanning provides insights into the potential impact of vulnerabilities on business operations, helping organizations make informed decisions about resource allocation and risk mitigation strategies without having the most in-depth and up-to-date cyberthreat intelligence. By automating the vulnerability scanning process, the reliance on manual intervention is reduced. This allows an organization to initiate more frequent and comprehensive scans, improving security posture as a whole.

An organization also needs solid risk assessments to identify the risk associated with each vulnerability it detects. AI-led risk assessments and prioritization can tackle that. An AI algorithm can potentially factor in various details on the vulnerability, how critical the system is, dependencies within the system, and the potential impact of exploitation. The algorithm can then assign a risk score to that vulnerability, which can provide a more accurate representation of the risk landscape.

These concepts also apply to AI-powered code analysis tools that can be used to scan and analyze the current state of software code syntax and logic. The AI-code analysis tool can be used to identify bugs, errors, insecure practices, and potential vulnerabilities and where errors are likely to occur. AI tools can even utilize generative artificial intelligence (GenAI) to make recommendations on code and how to solve errors.

Large language models (LLMs) and natural language processing (NLP) help these AI algorithms facilitate the rapid extraction of insights from unstructured text, expediting threat analysis. They also help with understanding meaning, and intent, synthesizing data into a human-consumable format or summary. AI algorithms allow for chatbot interface or copilot, powered by LLMs and NLP, which can provide information or recommendations, based on the structure and status of current applications, systems, and environments [38].

2.3.3 DoD and Government AI Use Cases for Cybersecurity

This section details use cases that the U.S. Department of Homeland Security (DHS), U.S. Department of the Air Force (DAF), U.S. Space Force (USSF), U.S. Army Cyber Command (ARCYBER), Defense Technical Information Center (DTIC), and Cybersecurity and Infrastructure Security Agency (CISA) have for improving their cybersecurity posture using AI-enabled tools.

2.3.3.1 DHS: Commercial GenAI for Code Generation. DHS employees are permitted to use commercially available GenAI for code generation in day-to-day work. These tools can dynamically create usable code through plain-language prompts submitted by the user. They use NLP and LLM to produce code in many different programming languages and for a variety of tasks [39].

- AI Techniques Used: GenAI, ML, NLP
- Stage of System Development Life Cycle: Operation and Maintenance

2.3.3.2 DAF and USSF: Nonclassified Internet Protocol Generative Pretraining Transformer (NIPRGPT). On 10 June 2024, the DAF announced that it would be launching a GenAI chatbot called NIPRGPT that would be hosted on the Nonclassified Internet Protocol Router Network (known as NIPRNet). This common access card (commonly known as CAC)-enabled GenAI tool can answer questions and assist with tasks such as correspondence, code analysis and generation, and background papers, all within a secure computing environment. The NIPRGPT project is an opportunity to understand key metrics like computational efficiency, resource utilization, and security compliance [40].

Figure 4. NIPRGPT [41].

2.3.3.3 ARCYBER: Panoptic Junction. According to a *DefenseScoop* article by J. Harper [42]:

> ARCYBER is piloting an AI/ML platform that will enable scalable, continuous security monitoring of networks and platforms. It analyzes system compliance, threat intelligence, and streaming cyberevent data, which will enable advanced detection of adversary activity, malware, and anomalies at speeds that human analysts could not come close to. But not only is it fast, it’s agile. It is rapidly taking the pulse of networks and assimilating threat information simultaneously, protecting networks in real time. And it is performing these security assessments in the lens of what is most applicable to the specific architecture.

2.3.3.4 CISA. This section discusses the AI-enabled cyberuse cases of CISA, which includes: cyberincident reporting and cyberthreat intelligence feed correlation, advanced network anomaly and SIEM-alerting models, critical infrastructure anomaly alerting, cybervulnerability reporting, advanced analytic-enabled forensic investigation, automated indicator sharing (AIS) and automated personally identifiable information (PII) detection, and automated indicator sharing scoring and feedback (AS&F).

- Cyberincident Reporting and Cyberthreat Intelligence Feed Correlation: Cyberthreat intelligence feed correlation uses AI-enabled capabilities to provide accelerated correlation across multiple incoming information feeds. This enables more timely enrichment to improve the externally shared information feeds. AI allows the algorithm to use the information items and results to learn the most efficient ways to perform the task. Additionally, tailored algorithms could be created to provide sustained surveillance of threat actor Tactics, Techniques, and Procedures [39].
    - AI Techniques Used: ML, NLP
    - Stage of System Development Life Cycle: Initiation
- Advanced Network Anomaly and SIEM-Alerting Models: Threat-hunting and SOC analysts are provided with terabytes per day of log data. Manually developed detection alerts and automatic correlation in SIEM are common but not comprehensive. Many cyberattacks can be probabilistically determined given sufficient training data and time. Analysts use automated tooling to further refine the alerts they receive and produce additional automated alerts based on aggregated information and curated subject matter expertise. This tooling provides CISA analysts with the capabilities to comb through data in an automated fashion with mathematically and probabilistically based models to ensure high-fidelity anomalies are detected in a timely manner [39].
    - AI Techniques Used: ML
    - Stage of System Development Life Cycle: Initiation
- Critical Infrastructure Anomaly Alerting: The CyberSentry program provides monitoring of critical infrastructure networks. Within the program, threat-hunting analysts require advanced anomaly detection and ML capabilities to examine multimodal cyberphysical data on IT and operational technology networks, including Industrial Control System and Supervisory Control and Data Acquisition (better known as ICS/SCADA). The critical infrastructure anomaly alerting model provides AI assistance in processing this information.

  - AI Techniques Used: ML, Visualization
  - Stage of System Development Life Cycle: Initiation

- Cybervulnerability Reporting: Vulnerability analysts require advanced automation tools to process data received through various vulnerability reporting channels, as well as aggregate the information for automated sharing. These tools leverage ML and NLP to increase the accuracy and relevance of data that are filtered and presented to human analysts and decision-makers. ML techniques also assist with aggregating the information in reports for presentation and further analysis. This includes data in the Know Exploited Vulnerabilities Catalog and the Common Vulnerabilities and Exposures system databases (better known as KEV and CVE, respectively).

  - AI Techniques Used: NLP, Visualization
  - Stage of System Development Life Cycle: Initiation

- Advanced Analytic-Enabled Forensic Investigation: CISA deploys forensic specialists to analyze cyberevents at Federal Civilian Executive Branch departments and agencies, as well as other state, local, tribal, territorial, and critical infrastructure partners. Forensic analysts can utilize advanced analytic tooling in the form of AI implementations to better understand anomalies and potential threats. This tooling provides forensic specialists with the capabilities to comb through data in an automated fashion with mathematically and probabilistically based models to ensure high-fidelity anomalies are detected in a timely manner.

  - AI Techniques Used: ML
  - Stage of System Development Life Cycle: Initiation

- AIS Automated PII Detection: CISA's automated PII detection and human review process incorporates descriptive, predictive, and prescriptive analytics. Automated PII detection leverages NLP tasks, including named entity recognition coupled with privacy guidance thresholds to automatically detect potential PII from within automated indicator sharing submissions. If submissions are flagged for possible PII, the submission will be queued for human review, where the analysts will be provided with the submission and AI-assisted guidance to the specific PII concerns. Within human review, analysts can confirm/deny proper identification of PII and redact the information (if needed). Privacy experts are also able to review the actions of the system and analysts to ensure proper performance of the entire process and provide feedback to the system and analysts for process improvements (if needed). The system learns from feedback from the analysts and privacy experts.

Through the incorporation of automated PII detection, CISA complies with privacy, civil rights, and civil liberties requirements of the "Cybersecurity Information Sharing Act of 2015" [43] and scaled analyst review of submissions by removing false positives and providing guidance of the submission to be reviewed. Through continual audits, CISA will maintain integrity and trust in system and human processes.

- AI Techniques Used: NLP
- Stage of System Development Life Cycle: Operation and Maintenance

- AS&F: AIS, a CISA capability, enables the real-time exchange of machine-readable cyberthreat indicators and defensive measures to help protect against and ultimately reduce the prevalence of cyberincidents. AIS is offered as part of CISA's broad authority to share information relating to cybersecurity risks, including authority to receive, analyze, and disseminate information. It fulfills CISA's obligation under the "Cybersecurity Information Sharing Act of 2015" [43] to establish and operate the federal government's capability and process for receiving cyberthreat indicators and defensive measures and to further share this information with certain other agencies, in some cases in a real-time manner.

  AS&F, built on the AIS Scoring Framework, defines an algorithm by which organizations can enrich Structured Threat Information Expression Indicator objects, shared via AIS, with (1) an opinion value that provides an assessment of whether or not the information can be corroborated with other sources available to the entity submitting the opinion and (2) a confidence score that states the submitter's confidence in the correctness of information they submit into AIS. When leveraged by CISA, AS&F uses AI/ML to perform descriptive analytics from organizational-centric intelligence to support confidence and opinion classification of indicators of compromise. Together, these enrichments can help those receiving information from AIS prioritize actioning and investigating Indicator objects.

  - AI Techniques Used: Descriptive Analysis, ML, NLP
  - Stage of System Development Life Cycle: Operation and Maintenance

2.3.3.5 DTIC: Threat Network Detection. The Defense Innovative Unit "partnered with the Army and DTIC to launch the AI-Based Knowledge Graphing project in 2019. The project aimed to develop a customized ML platform to rapidly ingest, analyze, visualize, and generate reports of strategic threat activity from open-source, web-based content" [22].

Using the dMetrics platform, DTIC was able to successfully develop [22]:

> …new capabilities, such as near-real-time alerts for specific behaviors and the identification of early indicators of adversarial network activity, to support DoD analysts. The platform allows DoD analysts to create personalized ML agents that continuously scan big datasets to identify and extract entities, actions, and relationships relevant to each analyst's area of responsibility.

3.0 Conclusions

While AI-enabled cybersecurity tools still have a lot of room for improvement and are not the all-in-one solutions that can solve all small businesses' cyberneeds, they can certainly bridge the many cybersecurity gaps they face on a regular basis. AI-driven cybersecurity tools can process huge amounts of complex structured and unstructured datasets, provide a holistic view of threat environment, respond quickly with real-time threat detection, reduce false positives, anticipate potential cyberevents or incidents, and provide actionable insight and recommendations on next steps. These qualities of AI-driven analytics in cybersecurity can lessen the burden small businesses have when trying to tackle their own cybersecurity risks. AI-enabled solutions have the potential to allow smaller cybersecurity teams to handle more incoming data and alerts, prioritize tasks, and rely less on manual input. This can aid in limiting alert fatigue and data overload, making day-to-day operations easier to digest. AI-driven cybersecurity platforms can incorporate up-to-date threat intelligence feeds into their algorithms to keep things current and promote information sharing withing the cybercommunity. These cybersecurity tools with AI-enabled features may provide a better bang for your buck, compared to those without those features, along with more robust solutions. Finally, AI-driven behavioral analytics allows for the detection of deviations from baseline standard operations. This provides a route for organizations to defend against unseen threats, malware, and zero-day exploits, which helps bridge that gap between cyberdefenses and adversaries.

References

[1] Hait, A. “The Majority of U.S. Businesses Have Fewer Than Five Employees.” The Pine Tree.net, https://new.thepinetree.net/?p=113247, 19 January 2021.

[2] Main, K. “Small Business Statistics of 2024.” Forbes Advisor, https://www.forbes.com/advisor/business/small-business-statistics/#sources_section, 31 January 2024.

[3] U.S. Small Business Administration Office of Advocacy. “Frequently Asked Questions About Small Business, 2023.” https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/, 7 March 2023.

[4] Owens, D. B., N. K. Cherry, and G. J. Duffy. “Comments of WTA: Advocates for Rural Broadband” Federal Communications Commission Docket no. 130909789-3789-01, U.S. Department of Commerce, National Institute of Standards and Technology, https://www.nist.gov/system/files/documents/2017/06/09/20131213_derrick_owens_wta_part1.pdf, 13 December 2013.

[5] Envizion IT. “Small Business Cyber Security Statistics.” https://envizionit.com/small-business-cyber-security-statistics/, 9 March 2023.

[6] Wronski, L. “CNBC|SurveyMonkey Small Business Index Q2 2022” Survey Monkey, https://www.surveymonkey.com/curiosity/cnbc-small-business-q2-2022/, 25 April 2022.

[7] Hiscox Inc. “Cyber Attacks Cost U.S. Small Businesses Over $8,000 Annually, Reveals Hiscox Cyber Readiness Report 2023.” Hiscox, https://www.hiscox.com/articles/cyber-attacks-cost-us-small-businesses-over-8000-annually-reveals-hiscox-cyber-readiness, 5 December 2023.

[8] Godziszewski, A. “2022 Study: 50% of SMBs Have a Cybersecurity Plan in Place.” UpCity, https://upcity.com/experts/small-business-cybersecurity-survey/, 2 May 2022.

[9] Duarte, F. “Amount of Data Created Daily.” Exploding Topics, https://explodingtopics.com/blog/data-generated-per-day, 13 June 2024.

[10] Verizon. “2024 Data Breach Investigations Report.” Verizon Business, https://www.verizon.com/business/en-gb/resources/reports/dbir/, 1 May 2024.

[11] Swain, G. "Hackers Leak Documents Stolen From Pentagon Contractor Leidos." CSO, https://www.csoonline.com/article/3477035/hackers-leak-documents-stolen-from-pentagon-contractor-leidos.html, 24 July 2024.

[12] Ross, R., V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST, NIST-SP 800-171, Revision 2, https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final, 14 May 2024.

[13] U.S. Department of Defense. "Safeguarding Covered Defense Information and Cyber Incident Reporting." Acquisition.gov, DFARS 252.204-7012, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting., 18 December 2024.

[14] Ross, R., V. Pillitteri, G. Guissanie, R. Wagner, R. Graubart, and D. Bodeau. "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement for NIST Special Publication 800-171." NIST, NIST-SP 800-172, https://csrc.nist.gov/pubs/sp/800/172/final, February 2021.

[15] Federal Acquisition Policy Division of the General Services Administration, U.S. Department of Defense, and National Aeronautics and Space Administration. "Basic Safeguarding of Covered Contractor Information Systems." Acquisition.gov, FAR 52.204-21, https://www.acquisition.gov/far/52.204-21, accessed November 2024.

[16] Chief Information Officer, U.S. Department of Defense. "About CMMC." DODCIO, https://dodcio.defense.gov/cmmc/About/, accessed November 2024.

[17] Lopez, C.T. "DoD Simplifies Process for Defense Contractors to Comply With Cybersecurity Rules.“ DoD News, https://www.defense.gov/News/News-Stories/Article/Article/3938314/dod-simplifies-process-for-defense-contractors-to-comply-with-cybersecurity-rul/, 17 October 2024.

[18] Summit 7 Leadership. "CMMC Compliance Deadline: When Do I Need to Be CMMC Compliant?" Summit 7, https://www.summit7.us/blog/cmmc-compliance-deadline#:~:text=Companies%20looking%20to%20become%20compliant,the%207%20Steps%20of%20CMMC, 16 October 2024.

[19] FedRAMP. "Program Basics." https://www.fedramp.gov/program-basics/, accessed on 30 October 2024.

[20] Stryker, C. “What Is AI Analytics?” IBM, https://www.ibm.com/think/topics/ai-analytics, 5 August 2024.

[21] Stanham, L. “What Is AI-Powered Behavioral Analysis in Cybersecurity.” CrowdStrike, https://www.crowdstrike.com/cybersecurity-101/secops/ai-powered-behavioral-analysis/, 7 September 2023.

[22] Defense Innovation Unit. “Machine-Learning Powered Platform Provides DoD Ability to Identify Threat Network Activity.” https://www.diu.mil/latest/machine-learning-powered-platform-provides-dod-ability-to-identify-threat, 30 October 2024.

[23] IBM. “What Is an Intrusion Detection System (IDS)?” https://www.ibm.com/topics/intrusion-detection-system, accessed on 30 October 2024.

[24] IBM. “What Is an Intrusion Prevention System (IPS)?” https://www.ibm.com/topics/intrusion-prevention-system, accessed on 30 October 2024.

[25] National Institute of Standards and Technology Computer Security Resource Center. “Glossary: Firewall.” NIST, https://csrc.nist.gov/glossary/term/firewall, accessed on 30 October 2024.

[26] Palo Alto Networks. “What Is Network Detection and Response (NDR)?” https://www.paloaltonetworks.com/cyberpedia/what-is-network-detection-and-response, accessed on 30 October 2024.

[27] Aarness, A. “What Is Endpoint Detection and Response (EDR)?” CrowdStrike, https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/, 26 October 2023.

[28] NetWitness LLC. “The Language of Cybersecurity: EDR vs. XDR.” NetWitness, https://www.netwitness.com/blog/edr-vs-xdr/, 15 September 2023.

[29] Palo Alto Networks. “What Is the Difference Between XDR vs. SIEM?” https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem, accessed on 30 October 2024.

[30] IBM. “What Is SOAR (Security Orchestration, Automation and Response)?” https://www.ibm.com/topics/security-orchestration-automation-response, accessed on 30 October 2024.

[31] Hayes, N. "Managed Detection and Response (MDR)." CrowdStrike, https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr/, 17 January 2024.

[32] Thiemann, T. "The Limitations of Traditional MDR: Why You Should Upgrade." ReliaQuest, https://www.reliaquest.com/blog/beyond-traditional-mdr/, 10 January 2023.

[33] Palo Alto Networks. "What Is a Threat Intelligence Platform (TIP)?" Cortex, https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform, accessed on 30 October 2024.

[34] McCarty, B. "Four Common Threat Intelligence Challenges and How to Overcome Them." Forbes, https://www.forbes.com/councils/forbestechcouncil/2023/12/05/four-common-threat-intelligence-challenges-and-how-to-overcome-them/, 5 December 2023.

[35] Balbix, Inc. "The Best Vulnerability Scanner Tools." Balbix, https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/, 25 October 2024.

[36] Hughes, B. "Cyber Operator." 315th Airlift Wing, VIRIN: 201013-Z-YE885-001A, https://www.315aw.afrc.af.mil/News/Photos/igphoto/2002539150/, accessed on 17 March 2025.

[37] Megasis Network. "AI-Powered Vulnerability Management: Identify and Prioritizing Risks." Medium, https://megasisnetwork.medium.com/ai-powered-vulnerability-management-identifying-and-prioritizing-risks-6b7308ecf3db, 4 April 2024.

[38] Cassestto, O. "AI SOC: The Definition and Components of AI-Driven SOC." Radiant Security, https://radiantsecurity.ai/learn/ai-driven-soc/, 10 June 2024.

[39] U.S. Department of Homeland Security. "Artificial Intelligence Use Case Inventory." https://www.dhs.gov/data/AI_inventory, accessed on 16 August 2024.

[40] Secretary of the Air Force Public Affairs. "Department of the Air Force Launches NIPRGPT." Air Force, https://www.af.mil/News/Article-Display/Article/3800809/department-of-the-air-force-launches-niprgpt/, 10 June 2024.

[41] Dark Saber. "NIPRGPT." https://devilops.mil/, accessed on 30 October 2024

[42] Harper, J. “Cybercom Seeing Successes With Panoptic Junction Artificial Intelligence Capability.” *DefenseScoop*, https://defensescoop.com/2024/10/30/cybercom-army-cyber-command-panoptic-junction-artificial-intelligence/, 30 October 2024.

[43] 114th U.S. Congress. “Cybersecurity Information Sharing Act of 2015.” S.754, U.S. Government Publishing Office Washington, DC, https://www.congress.gov/bill/114th-congress/senate-bill/754, 2015.

Biography

Olutoye Sekiteri works with the Cybersecurity & Information Systems Information Analysis Center (CSIAC) as a research analyst. He provides research efforts related to CSIAC's four technical focus areas, conducts data analysis to support U.S. Department of Defense science and technology communities, and connects government clients with subject matter experts to aid in answering technical inquiries. Mr. Sekiteri obtained a B.S. in information systems from the University of Maryland, Baltimore County (UMBC), where he is also currently pursuing a master's degree in Cybersecurity. At UMBC, he worked as a research assistant for its Department of Information Systems, supporting a research project recording emergency medical technician stress levels during interactive simulations.