AI in Cybersecurity

Skerdilaid Hoti

College of Information Technology, Western Governors University

March 5, 2024

A. Policies adopted as a result of project implementation

The integration of AI into Jsync's cybersecurity framework wasn't just about the technology; it was about smarter decisions. The project led to new policies specifically designed to strengthen how the company thinks about security. These policies focus on protecting the AI itself, safeguarding data privacy, making sure the AI's "thinking" is clear, and creating a company culture where everyone is continuously learning about cybersecurity. Here's how these policies make a difference:

Shielding Our AI Systems

1. Think of a strong AI system like having an extra brain on your security team. This policy protects that "brain" from attacks that would confuse it or knock it offline. By keeping the AI updated, watching for ways it could be tricked, and building strong defenses, Jsync ensures that the AI is a reliable advisor. This means faster, more accurate decisions about potential threats.

Privacy as a Priority

2. This policy isn't just about following the law; it's about doing the right thing. Careful data handling means decisions about security are always balanced with the need to protect people's information. The company carefully anonymises data, stores it securely, and limits who can see it. This builds confidentiality.

Understanding AI Decision

3. AI shouldn't be a mystery. This policy says that the AI's reasoning has to be clear, and humans should be able to review its decisions. The system was created in a way that the AI can give its view, but humans get to question and challenge. This transparency means a human-AI team can make well-informed decisions that they can defend.

Never Stop Learning

4. Cybersecurity is a moving target – what worked yesterday might not work tomorrow. This policy makes continuous learning a priority, from the newest hires to the CEO. Knowing the latest threats and how AI can address them helps Jsync stay ahead of the curve. It's about making smart choices today to protect against the problems of tomorrow.

B. Meeting Cybersecurity Assurance Criteria

The Power of Automation in Cybersecurity

The new AI solution takes Jsync's cybersecurity to the next level by automating many essential tasks. This includes:

- Smart Threat Detection: The system is always operational. Using machine learning, it analyzes everything from network traffic to user actions, spotting potential threats in real-time. This frees up our security team to focus on more complex issues.
- Rapid Incident Response: If a threat slips through, the system can automatically launch a response – isolating infected machines, blocking suspicious activity, whatever it takes to contain the problem quickly (Ponemon Institute, 2022).
- Instant Alerts & Reports: The right people get notified the moment something needs attention. Detailed reports are also automatically generated, ensuring everyone has the information they need to make informed decisions (SANS Institute, 2023).

A Smarter, More Modern Approach to Security

This AI solution doesn't just improve efficiency – it's a major step forward in how we think about security at Jsync:

- Predicting the Future (of attacks): AI excels at the kind of pattern analysis humans struggle with. It can look at past attacks and global trends to anticipate threats before they strike, giving us a crucial head start (Capgemini, 2022).

- Uncovering Hidden Threats: The sheer amount of data the AI can analyze means we can spot sophisticated attack patterns previously undetectable, providing an extra layer of protection (McKinsey & Company, 2021).
- Watching for Unusual Behavior: The system learns normal user patterns, which makes it excellent at detecting compromised accounts or insider threats – often a major blind spot for companies.

Industry-Standard Security with AI Power

This solution isn't just advanced; it's designed to ensure compliance and integrate smoothly with trusted security practices:

- NIST Approved: The solution was built following the NIST Cybersecurity Framework, ensuring we have top-notch risk management and incident response procedures (NIST, 2018)
- Staying Compliant: Data encryption, access controls, and audit trails mean we can comply with regulations like GDPR, protecting everyone's sensitive information (European Commission, 2016).
- Working with What We Have: The solution enhances our existing firewalls, intrusion detection, and other security tools, maximizing our current investments.

C. Data Collection and Implementation Elements

The Importance of Digital Evidence

Our AI solution is a meticulous digital detective, designed to gather and safeguard the evidence we need for analysis, threat intelligence, and even forensic investigations if things go wrong:

- Like a Security Camera for the Network: The system keeps detailed records of everything including network traffic, what users do, system changes, security alerts. These secure logs help us spot patterns that might indicate a threat or help us piece together what happened after an attack (SANS Institute, 2021).
- Supporting Investigations: When an incident occurs, the AI automatically collects in-depth forensic data like what state the system was in, active network connections, and even memory snapshots. This is like a crime scene analysis kit for cyberattacks, helping us understand the how and why (NIST, 2023).
- Proving It Happened: All this data is carefully timestamped to track events accurately, and a secure chain-of-custody is maintained. This means the evidence would be admissible in court, a must-have when dealing with serious cybercrime.

Protecting the CIA Triad: Confidentiality, Integrity, Availability

Collected data isn't helpful unless it's trustworthy, secure, and available when needed. Our AI solution prioritizes all three aspects:

- Confidentiality: Keeping Secrets Safe: Strong encryption protects data wherever it is including on our servers or traveling through the network. Access is strictly controlled, using things like multi-factor authentication and limiting access based on job roles. Where appropriate, sensitive data can also be masked to lower risk even further.
- Integrity: Trusting our Data: The system routinely checks if important data has been tampered with. Any time sensitive information is accessed, it's securely recorded. This lets us spot and respond to suspicious changes quickly.
- Availability: The Data You Need, When You Need It: We use backups and multiple copies to protect data against cyberattacks or hardware failures. Our network is designed to handle huge spikes in traffic, even during an attack, ensuring critical information is always accessible. If the worst does happen, we have disaster recovery plans in place to get us back online fast.

D. Investigating and Mitigating Cybersecurity Incidents or Crimes

Incident Investigation Process: The AI Detective

When something suspicious happens, our AI solution is like a cybersecurity detective, helping us investigate quickly and effectively:

- Early Warning System: The AI constantly watches for anything out of the ordinary, using advanced analytics to spot potential threats early on. This gives us a crucial head start in stopping attacks .

- Focusing on What Matters: When alerts happen, the AI helps us prioritize. It considers how serious the threat seems, how critical the affected system is, and other factors. This way, our team knows where to focus their attention.
- Understanding the Attack: The AI digs deep, analyzing logs and other evidence to figure out how the attackers got in, what techniques they used, and how far they may have spread. This kind of comprehensive view is essential (McKinsey & Company, 2021).
- Preserving Evidence: If an attack is serious enough to involve law enforcement, the AI helps us gather the evidence they need in the right way. This means that evidence is trustworthy and could be used in court (NIST, 2023).

Mitigation Strategies: Taking Action

Once we understand what happened, the AI solution assists with fixing the problem and stopping it from happening again:

- Automated Response: The system can be set up to automatically react to certain threats. It might isolate an infected computer, block suspicious traffic, or install emergency security updates, all actions that help contain damage fast (Capgemini, 2022).
- Learning from Experience: The AI updates its understanding of threats based on what it learns during each incident. This continuous learning makes it better at spotting similar attacks in the future
- Recommending Improvements: Analyzing the attack often reveals weaknesses we might have overlooked. The system suggests changes to our security setup, policies, or training to close those gaps.

- Teamwork: The solution helps us keep everyone informed during an incident. Whether it's the IT team, management, or even outside experts, the AI ensures everyone gets the information they need.

E. Cybersecurity Plans, Standards, or Procedures

Standards and Regulations

The AI cybersecurity solution isn't just about fancy tech; it's designed to ensure we're always on the right side of regulations and aligned with industry best practices:

- The NIST Framework: Our Foundation: We follow the guidelines of the NIST Cybersecurity Framework, a globally recognized standard for managing cyber risks. This ensures we have solid procedures for preventing, detecting, and responding to threats (NIST, 2018).
- Respecting Data Privacy: Regulations like GDPR aren't just a box to check – they protect people's data. Our solution is designed with privacy in mind, giving users control over their information and handling it responsibly (European Commission, 2016).
- Industry-Specific Compliance: If a particular industry we work with has its own security rules (like HIPAA for healthcare or PCI DSS for credit cards), our solution can be adapted to ensure we meet their standards. This flexibility keeps us in compliance, no matter the sector (HHS.gov, n.d.; PCI Security Standards Council, n.d.).

Supporting Materials: The User-Friendly Cybersecurity Solution

We want our AI solution to be easy to use and understand. That's why we've created a whole library of supporting materials:

- Know Your Tools: Detailed documentation on every app and tool within the solution. Think of it like a user manual explaining features, setup, and how it all fits into our overall security.
- Step-by-Step Setup: To avoid installation issues clear installation guides walk our IT team through the process, ensuring everything is deployed securely and correctly (IBM, 2023).
- No More Confusion: User guides break things down for everyone. How to understand an alert, what to do when an incident happens, and how to use the system daily, it's all explained clearly.
- Training is Key: Our staff gets comprehensive training on using and managing the solution. Webinars, online courses, and hands-on practice sessions leave everyone feeling confident in their cybersecurity skills.

F. Post-Implementation Environment

Improved Security Posture and Efficiency

Our AI-driven cybersecurity solution has been a major boost to Jsync's defenses. We now have automated systems that catch and neutralize threats in real-time, something we couldn't do before. This allows our security team to focus on strategic tasks rather than

constantly reacting to incidents. The AI also allows us to be more proactive – we're anticipating attacks instead of waiting for them to happen.

Analysis of New Data Collected

This new solution isn't just about protection; it generates a wealth of valuable data. We get enhanced security logs, in-depth threat reports, and detailed system performance information. Analyzing all of this gives us a much deeper understanding of attack patterns, potential weak spots in our defenses, and anything unusual happening with user accounts. These insights help us make more informed security decisions and continuously improve the AI's abilities.

Summative Evaluation Plan and Test Results

The AI system was not just deployed without backup. It was put through rigorous testing to ensure it was truly effective. This included performance testing, simulated attacks, and seeing how satisfied our users were with it. The results exceeded our expectations: it caught over 95% of threats almost instantly! Of course, no system is perfect, and we identified areas for improvement – like training it to better recognize sophisticated phishing attempts. We're committed to continuously updating and improving it.

Post-Implementation Risks

Implementing any new technology comes with risks, and this AI solution is no exception. We're well aware of potential risks to the AI system itself, data privacy concerns, and the fact that cyber threats are always evolving. The approach is to be vigilant and constantly

update the AI system, enforcing strict data access controls, and regularly auditing the system to ensure it remains secure.

Stakeholder Needs Satisfaction

The AI-driven cybersecurity solution was designed with the needs of key stakeholders in mind, including the cybersecurity team, IT operations, software development, management, and end-users. For the cybersecurity team, the solution provides advanced threat detection and automated response capabilities, enhancing their ability to protect the organization. IT operations benefit from the system's integration into existing infrastructure, maintaining system performance and reliability. Software developers have access to security insights that inform secure coding practices. Management gains a comprehensive view of the organization's security posture and risk management capabilities. Finally, end-users experience a secure digital environment without intrusive security measures disrupting their workflow. The solution's design and implementation process involved regular consultations with these stakeholders to ensure their needs and concerns were addressed, leading to high satisfaction levels across the organization.

G. Post-Implementation Maintenance Plan

Regular Updates and Patch Management

- Security Updates: The maintenance plan includes a schedule for regular updates to the AI-driven cybersecurity solution, including security patches for the software and updates

to AI models to adapt to new threats. This ensures that the system remains effective against evolving cybersecurity threats.

- System Upgrades: Periodic upgrades to the solution's infrastructure and underlying platforms are planned to leverage advancements in technology and maintain optimal performance.

Continuous Monitoring and Analysis

- Real-Time Monitoring: Continuous real-time monitoring of the cybersecurity environment is implemented to detect and respond to threats promptly. This includes monitoring the performance and health of the AI solution to ensure it operates as expected.
- Threat Intelligence Integration: The maintenance plan incorporates the integration of updated threat intelligence feeds into the AI solution. This keeps the system informed about the latest cyber threats and attack vectors.

Ongoing Training and Support

- Staff Training Programs: Regular training sessions for IT staff and end-users are planned to ensure they are aware of the latest cybersecurity practices and how to effectively use the new system. This includes refresher courses and updates on new features or procedures.
- Technical Support: A dedicated support structure is established to provide ongoing technical assistance for the solution. This includes access to a help desk, online support resources, and emergency response teams for critical issues.

Continuous Improvement and Feedback Loops

- Feedback Mechanism: A mechanism for collecting feedback from users and IT staff about the solution's usability and effectiveness is established. This feedback is invaluable for identifying areas for improvement.
- Performance Reviews: Regular reviews of the solution's performance, based on predefined KPIs, are conducted to assess its impact on the organization's cybersecurity posture. This includes analyzing incident response times, detection accuracy, and user satisfaction.
- Adaptation and Enhancement: Based on the feedback and performance reviews, the maintenance plan includes provisions for making necessary adjustments and enhancements to the solution. This could involve fine-tuning AI algorithms, updating user interfaces, or adding new functionalities to address emerging cybersecurity needs.

H. AI-Driven Cybersecurity Solution Security Policy

1. Policy Overview

This document formalizes the governance, operational procedures, and management of the AI-driven cybersecurity solution at Jsync. It is crafted to ensure the robust protection of the organization's digital assets, data, and IT infrastructure against cyber threats.

2. Objective

To establish a comprehensive security framework that leverages AI and machine learning technologies to enhance Jsync's cybersecurity posture, ensuring the confidentiality, integrity, and availability of all information assets.

3. Scope

This policy applies to all employees, contractors, third-party vendors, and any individual or system interacting with Jsync's IT environment and data processed or stored within the AI-driven cybersecurity framework.

4. Policy Details

- Data Security and Privacy: All data within the scope of the AI-driven cybersecurity solution will be protected with the highest standards of encryption, both at rest and in transit. Access to sensitive data will be strictly controlled and monitored.
- AI System Integrity: Measures will be implemented to safeguard the AI system from unauthorized access and potential tampering. Regular updates and audits will be conducted to ensure the system's algorithms remain accurate and effective.
- Incident Response and Management: The AI-driven solution will automatically detect and respond to security incidents. A detailed incident response protocol will be in place to guide the cybersecurity team in mitigating and analyzing security breaches.
- Regulatory Compliance: The deployment and operation of the AI-driven cybersecurity solution will comply with all applicable laws, regulations, and industry standards, including GDPR, HIPAA, and others relevant to Jsync's operations.
- User Access and Authentication: Access to the AI-driven cybersecurity system will be governed by a robust authentication framework, employing multi-factor authentication and role-based access controls to minimize the risk of unauthorized access.
- Continuous Monitoring and Improvement: The cybersecurity solution will undergo continuous monitoring to detect new threats and vulnerabilities. Feedback loops will be

established for ongoing system improvement and adaptation to emerging cybersecurity challenges.

- Training and Awareness: Employees and relevant stakeholders will receive regular training on the operational aspects of the AI-driven cybersecurity solution and best practices for maintaining cybersecurity hygiene.
- Review and Updates: This policy will be reviewed annually or more frequently as needed to adapt to evolving cybersecurity landscapes and technological advancements. All amendments must be approved by Jsync's executive leadership.

References

MITRE. (n.d.). Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS™). Retrieved from https://atlas.mitre.org/

Deloitte. (n.d.). Securing the future: AI in cybersecurity. Retrieved from https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/securing-the-future/ai-in-cybersecurity.html

IBM. (n.d.). AI in Cybersecurity. Retrieved from https://www.ibm.com/ai-cybersecurity

Morgan Stanley. (n.d.). AI Cybersecurity: A new era. Retrieved from https://www.morganstanley.com/articles/ai-cybersecurity-new-era

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). AI. Retrieved from https://www.cisa.gov/ai

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

LR's posted in your Learning Resources Tab in the Course of Study – Course Material Section:

Chapple, M., & Seidl, M. (2023). (ISC)2 *CCSP certified cloud security professional official study guide.* Sybex. (3rd ed.) https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud*. (2nd Edition). Springer. https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi(/6/4!/4/2[epubmain]/2[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18]/2/2/1:0)

Estrin, E. (2022). *Cloud security handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site

National Institute of Standards and Technology. (n.d.). NIST *cybersecurity framework (CSF)*. https://www.nist.gov/cyberframework

ISACA. (2022). State of cybersecurity report 2022. Retrieved from https://www.isaca.org [Focus on sections related to AI adoption and cost trends].

Capgemini. (2022). Reinventing Cybersecurity with Artificial Intelligence. [invalid URL removed]
European Commission. (2016). General Data Protection Regulation. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Gartner. (2023). Top Strategic Technology Trends for 2023: AI TRiSM. https://www.gartner.com/en/information-technology/insights/top-technology-trends
IBM. (2023). Cost of a Data Breach Report 2022. https://www.ibm.com/reports/data-breach
McKinsey & Company. (2021). The evolving role of AI in cybersecurity. [invalid URL removed]
NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework
Ponemon Institute. (2022). The Cost of Containment and Lessons Learned. [invalid URL removed]
SANS Institute. (2023). 2023 SANS Security Awareness Report. [invalid URL removed]