Strategy and Innovation Paper

A Capstone Paper

An individual paper written by:

Amari (AJ) Jones

Focus

Industry: Cybersecurity

Role/Job Title: Security Analyst (leading to Cyber Threat Intelligence Analyst)

Cybersecurity is an expansive and one of the most dynamic industries in today's economy (Jonker et al., 2025). From AI-driven threats, ransomware, and the expansion of cloud infrastructure, these make cybersecurity a key to overall risk management and become a part of business impact analytics. This industry has also made an impact on government level with policies and acts coming to play like the Payment Card Industry Data Security Standard (PCI DSS), Family Educational Rights and Privacy Act (FERPA), and the General Data Protection Regulation (GDPR) in Europe.

The Security Analyst role serves as an entry point of the industry, with responsibilities spanning to monitoring, detection, initial incident response, and fine tuning business impact analysis and disaster plans. As Artificial Intelligence grows more advanced, this role is evolving towards and revolutionizing threat detection, automated responses, and strengthening vulnerability management. AI in this field should be used as a tool for the overarching form of Information Security and also scale down to analyzing behaviors, detecting phishing, and firewall enhancements for a business. (*Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense*, n.d.)

Industry External Analysis

Threats of New Entrants – Medium

Cybersecurity is riddled with startup activity. Cloud-native companies emerge with niche solutions but they have to deal with the pool of start up problems such as high capital requirements, compliance laws and acts burdens, and customer trust barriers. With a *security* company, there must be trust because nobody simply throws their information, let alone their trust to companies and methods like Everyday-Low-Prices won't offer much of a solution because it leads to customers/clients questioning why the price is so low. This leads to already established players like CrowdStrike and Palo Alto Networks to have brand recognition and market dominance.

Bargaining Power of Suppliers – Medium

There are suppliers of specialized datasets on the web and AI tools hold some leverage, however they are paid for. Meanwhile, there are alternatives such as open-source frameworks like the MITRE ATT&CK, which lowers switching cost. Though, companies like CrowdStrike reduces dependence on it through in-house innovations like Falcon Intelligence. (*CrowdStrike Falcon® Adversary Intelligence Data Sheet*, n.d.)

Bargaining Power of Buyers – High

Enterprises and governments can switch vendors easily, and they demand competitive pricing. Companies like CrowdStrike combat this through long-term contracts and platform modularity, embedding into customer operations. (*Trusted Embedded OEM Partners* | *CrowdStrike*, n.d.)

Threats of Substitutes – Low

There are no replacements or substitutions for cybersecurity. Automation may reduce some manual tasks, but the concept and the overall demand continues to grow with the digital economy, with projection to grow twenty-nine percent (29%) within the next nine (9) years, which is much faster than average (Bureau of Labor Statistics, 2025).

Rivalry Among Competitors – High

A lot of cybersecurity and IT companies compete against each other like titans. Microsoft, SentinelOne, Palo Alto Networks, Cisco and more are in competition with each other. Frequent feature rollouts, aggressive marketing, and price competition intensify the rivalry.

Force	Scale	Rationale
Threat of New Entrants	Medium	Startups exist but scaling is low due to many requirements like trust, compliance and heavy capital.
Supplier Power	Medium	Vendors hold data leverage, solved by open-source tools.
Buyer Power	High	Buyers may have choices and can switch easily.
Substitutes	Low	Cybersecurity has no viable substitutions, and AI can only **assist** rather than replace.
Rivalry	High	Intense competition between leaders and disruptors.

Innovation Lens

Cybersecurity is a highly innovative market. It is shaped by constant adaptation to evolving threats in which its index grows by the day as attackers and defenders find new methods to perform their job. This shows how resources like MITRE ATT&CK versions are updated twice a year. (*Version History | MITRE ATT&CK®*, n.d.)

Looking at the industry from a "Novelty, Useful, Implemented" test's lens, Cybersecurity has proved itself to be a prominent figure head by the following.

Test Category	Test Result	Rationale
Novelty	Pass	Although Cybersecurity has been around for a long time, it still remains a novelty as it is constantly evolving with technology.
Useful	Pass	Cybersecurity has proved itself useful time and time again from analysis to the act of red teaming, forming a shield to protect a company and its employees.
Implemented	Pass	Cybersecurity is implemented everywhere, down to your email filtering out what is junk and what isn't. It is tool that companies should implement throughout all technological use.

Blue Ocean Strategy

Not everyone is a cybersecurity focused individual, and that is a given. There are many other things to focus on in the world of business like Finance, Marketing, Management, Accounting and many more departments within a company. However, they are all involved within Cybersecurity or protected by the latter mentioned industry as if it was an umbrella. Cybersecurity serves to protect information on company trade secrets and personal information of customers, ensuring their privacy.

Open and Free-Model Innovation

There are a lot of open-source technologies and software that can help ensure security in a business and there are a lot of forums where users can share their insights through frameworks (GitHub Repositories, MITRE ATT&CK, Global Threat Reports) which highlights collaboration across the industry.

High-End Disruptive Innovation

Artificial Intelligence has brute forced its way into the industry and shaken it at its core. From Security Analysts using AI to scan reports and use it as precedence to judge and suggest actions for the next problem, AI has also been used by the other end of the “good vs evil” trope that lies within Cybersecurity. Blackhat Hackers or Bad Actors have leveraged AI for deepfake phishing, automated exploit generations, and polymorphic malware. These

would disrupt legacy tools and create a necessity to implement new strategies, and creation of new tools.

Company Internal Analysis: CrowdStrike

The company chosen was CrowdStrike. As someone who wishes to enter the Cybersecurity realm, I'd like this company to be one of the few I'd work under or collaborate with. Through extensive searching through Form 10-K in 2024, I've identified a few strengths within the business.

Strengths

AI Leverage: CrowdStrike has already taken the initiative in using AI in its operations like the inclusion of Charlotte AI. This tool reduces an Analysts' work, allowing them to search through data with ease and reducing work time by 40+ hours a week.

Unified AI-native Platform: The use of a single AI agent and graph analytic platform enables consolidation, faster deployment, and reuse of data with ease.

Gaps

Dependence on Third-Party Infrastructure: Their use of AWS and Azure Cloud Services allows them to be at risk of being vulnerable whenever their Vendors are under any kind of trouble on their side (example: if AWS servers are down, what is to happen with other businesses using their services?).

Intense Competition: There is a lot of competition in Cybersecurity with there being a lot of vendors in EPP, XDR, and Cloud Security. This pressures win rates and pricing in deals.

CrowdStrike's Value Chain for 2024			
Primary Activities		**Supporting Activities**	
Inbound Logistics	Enriched threat graph, intel graph, and asset graph.	**Procurement**	Use of third-party data centers.
Outbound Logistics	SaaS delivery model. CrowdStrike stores.	**TechDev**	Continuous R&D in AI-native security, Charlotte AI and APIs.
Service	Incident response, forensics.	**Human Resources**	DEI Initiatives have been in place, remote-first culture, employee resource group.
		Infrastructure	Strong IP portfolio, governance and compliance functions.

CrowdStrike is already embedding AI across its platforms like Falcon, particularly through Charlotte AI, which is an assistant for analysts. Over the next three years, AI should further

automate detection and response, reduce false positive reports, and accelerating remediation.

AI Impact

Current Use

In cybersecurity today, some use cases of AI and its involvement include:

- **Identity and Access Management**: AI is used to understand patterns in user sign-in behaviors and understand infrequent behaviors. It is also used to force multi-factor authentication or password reset when conditions are met (example: resetting password after 72 days) (*What Is AI for Cybersecurity? | Microsoft Security*, n.d.).
- **Incident Investigation and Response**: During Incident Response, security professionals must sort through heaps of data to uncover potential cyberattacks. AI can help identify and correlate the most useful events across the data sources, making it a less timely process for the security analyst. (*What Is AI for Cybersecurity? | Microsoft Security*, n.d.).
- **Threat Detection and Prediction**: AI helps monitor endpoints, emails, identities, and cloud apps for infrequent behaviors, correlate incidents, and surface them to teams. AI models can also disrupt advanced attacks like ransomware and provide suggestions to provide coverage and perhaps save the company cost. The AI is also

used for threat intelligence, creating more proactive approaches to threats and risks. (*What Is AI for Cybersecurity? | Microsoft Security*, n.d.).

Three-Year Forecast

In three years, AI can do anything. We've already seen a lot of AI breakthroughs within the 2025 year by itself and for the Cybersecurity industry, we can predict the tool being used in a more hands on situation. AI red-teaming and AI-powered attack simulations can become standard. Regulation will grow around privacy and ethical use of AI. The role of Security Analyst can evolve from loge analysis to AI-supervised strategies where we will have to train the AI personally, manually sanitize datasets and give it to AI without proper study so the AI can do much more. But this requires new skills such as advanced Machine Learning knowledge, insurance of knowledge of the compliance acts and laws, and interpretation of AI outputs and proper AI prompt engineering. These skills will ensure that the Analysts can use new tools like Agentic AI like Charlotte AI, Threat AI, and more to automate high-impact workflows. (*Charlotte AI: Agentic Analyst for Cybersecurity*, n.d.)

Ethical and Regulatory Implications

AI in cybersecurity introduces an ethical dilemma. With AI being trained and we see it saving information that is being skewed around the generative AI platforms, and we never

know if the next information we see on its next output is our own. Cybersecurity in corporations increasingly relies on AI tools for threat detection, incident response and even employee-awareness simulations; but they are trained on massive datasets that could include personal or sensitive information collected whether intentionally or unintentionally via web scraping or other means. When data isn't anonymized, private information may be exposed or misused like medical photos being used in a public dataset for an image synthesis model (Owen-Jackson, 2025).

From a regulatory standpoint, laws and acts like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) serve as frameworks for ethical guidelines for anything and should be used for AI deployment even though they were developed prior to the rapid rise of generative AI. In a role base, Cyber Security Analysts must make sure to properly sanitize the data they put into the AI before they generate reports or perform any actions, and they must also balance efficiency along with accountability to make sure there are no false positives and biases do not perpetuate. This way, AI doesn't become something that takes the job, rather it becomes a tool that helps along the way.

Personal Evaluation

After considering what the role will have to offer pre and post this assignment and the thoughts of AI, my interest in the industry has strengthened through this project. AI isn't

eliminating analysts, if anything it's allowing them to take on more of the daunting tasks that require a human focus. CrowdStrike shows that they are leveraging technology and innovation that is being developed in our time so that the entire company can focus on more adversarial intelligence, focus on compliance laws and strategic overhead. This allows me to feel secure that cybersecurity is ultimately rewarding as a career path for me.

Tables and Figures

This section is a copy-paste of the tables used in the work piece above.

Five Forces Summary Table

Force	**Scale**	**Rationale**
Threat of New Entrants	Medium	Startups exist but scaling is low due to many requirements like trust, compliance and heavy capital.
Supplier Power	Medium	Vendors hold data leverage, solved by open-source tools.
Buyer Power	High	Buyers may have choices and can switch easily.
Substitutes	Low	Cybersecurity has no viable substitutions, and AI can only **assist** rather than replace.
Rivalry	High	Intense competition between leaders and disruptors.

CrowdStrike's Value Chain for 2024

Primary Activities		Supporting Activities	
Inbound Logistics	Enriched threat graph, intel graph, and asset graph.	**Procurement**	Use of third-party data centers.
Outbound Logistics	SaaS delivery model. CrowdStrike stores.	**TechDev**	Continuous R&D in AI-native security, Charlotte AI and APIs.
Service	Incident response, forensics.	**Human Resources**	DEI Initiatives have been in place, remote-first culture, employee resource group.
		Infrastructure	Strong IP portfolio, governance and compliance functions.

Novelty Useful Implemented Test Table

Test Category	Test Result	Rationale
Novelty	Pass	Although Cybersecurity has been around for a long time, it still remains a novelty as it is constantly evolving with technology.
Useful	Pass	Cybersecurity has proved itself useful time and time again from analysis to the act of red teaming, forming a shield to protect a company and its employees.
Implemented	Pass	Cybersecurity is implemented everywhere, down to your email filtering out what is junk and what isn't. It is tool that companies should implement throughout all technological use.

Work Cited

Artificial intelligence (AI) in cybersecurity: The future of threat defense. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Jonker, A., Lindemulder, G., & Kosinski, M. (2025, September 16). Cybersecurity. *IBM*. https://www.ibm.com/think/topics/cybersecurity

Lyman, V. (2024, December 2). *Will Cybersecurity be Replaced by AI? - UWF*. University of West Florida Online. https://onlinedegrees.uwf.edu/articles/cybersecurity-and-ai

Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, Information Security Analysts, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Trusted Embedded OEM Partners | CrowdStrike. (n.d.). https://www.crowdstrike.com/en-us/partner-program/embedded-oem

CrowdStrike Falcon® Adversary Intelligence Data Sheet. (n.d.). https://www.crowdstrike.com/en-us/resources/data-sheets/crowdstrike-falcon-adversary-intelligence

Version History | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/resources/versions

CrowdStrike Holdings, Inc. Form 10-K for the Fiscal Year Ended January 31, 2024. United States Securities and Exchange Commission, 7 Mar. 2024.

https://www.sec.gov/ix?doc=/Archives/edgar/data/1535527/000153552724000007/crwd-20240131.htm

What is AI for cybersecurity? | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity

Charlotte AI: Agentic Analyst for Cybersecurity. (n.d.). https://www.crowdstrike.com/en-us/platform/charlotte-ai

Owen-Jackson, C. (2025, April 17). Navigating the ethics of AI cybersecurity. *IBM*. https://www.ibm.com/think/insights/navigating-ethics-ai-cybersecurity

AI Usage

ChatGPT (GPT-5) was used for the following:

- The AI was used to help me narrow my thoughts and guide me towards the role I wanted.
- ChatGPT 5 was assisted in formatting my table.
- Helped in formatting my references.
- Generate ideas of structure of the paper to look neat (headers, sub headers).
- Gave me a few ideas of links to look at for CrowdStrike through its extensive website.
- Assisted with the Value Chain Table format (along with referring to the Case 3 Project).
- Used ChatGPT 5 to guide me to areas within CrowdStrike's 10-K form to save time in reading the file. https://chatgpt.com/share/68d21676-4528-8008-9c9c-0238d7bfd538