FIREEYE CASE STUDY

Team 7

Michael Schultz, Abdullah Shahid, Huy Tran, Jorge Vargas

George Mason University

IT 429 - Security Accreditation of Information Systems

Professor Hussna Azamy

November 23, 2025

Abstract

This paper will examine how FireEye integrated artificial intelligence into its operational model to address the growing speed, scale, and complexity of modern cyberthreats. The analysis discusses the type of projects most suitable for AI implementation, what FireEye's strategy was, why they adopted a Human + AI approach, and what key parameters are needed to successfully integrate AI into an organization. The paper also discusses the organizational requirements that enabled FireEye's analysts to adapt and make use of AI augmented workflows successfully, including training, cross collaboration, and use of an automatability spectrum framework to delineate human and machine roles. While adaptive machine learning represents a new challenge in terms of trust and oversight, it remains a continuation of long-standing efforts to improve scale and efficiency. Organizations are not in entirely uncharted territory, because frameworks such as NIST SP 800-37 and SP 800-53 already anticipate automated mechanisms paired with continuous monitoring, and human judgement and oversight.

Introduction (Abdullah)

Cybersecurity is now a priority, around the world. Governments, critical infrastructure operators and private organizations face more attacks every year and they all depend on security firms that can process enormous amounts of data, identify threats, and respond in real time. FireEye became a leader in this environment by using virtual machine sensors, human driven intelligence and large-scale detection tools (FireEye, 2019a). As widespread global adoption of cloud services, mobile platforms and connected networks have greatly expanded the attack surface, the traditional methods of cybersecurity could not keep up. FireEye changed from a hardware-based approach to a software and data-oriented model, which allowed FireEye to collect, centralize and analyze telemetry data at a global scale. Today, the firm has more than 17 million virtual machine sensors deployed and stops between 50,000 and 70,000 malicious events each hour, showing the necessity of an automated system with human oversight (FireEye, 2019b).

We will examine FireEye's development within this modern cybersecurity landscape, and how FireEye strengthened its capabilities with its Human + AI strategy. The analysis looks at how FireEye integrated machine learning into its security operations, how its Human + AI model allowed analysts to apply reasoning and judgment to machine generated outputs, and why these hybrid systems became necessary as adversaries grew more sophisticated. The 2020 FireEye breach demonstrated that even the most advanced organizations remain vulnerable to highly capable nation state attackers, and there is a need for continuous improvement in both AI based tools and human expertise (Reuters, 2020).

FireEye's evolution reflects the larger transformation within the modern cybersecurity industry, where the scale and evolution of cyberthreats demands that organizations automate the flow of data to free up human analysts to make decisions. FireEye's shift towards an integrated, organization-wide Human + AI strategy shows how organizations can adapt to new technological pressures and demands and make use of more capable forms of automation to guide and augment human decision making and response, rather than replace it.

Summary of the Case (Michael)

Global spending on cybersecurity reached $43.1 billion dollars in 2020, which shows how essential cybersecurity has become for governments and private organizations trying to defend themselves against increasingly advanced persistent digital threats (Statista, 2020). Additionally, projections show that worldwide cybersecurity expenditure will exceed $213 billion dollars in 2025, showing the rapid growth in five years in spending and investment to protect modern digital infrastructure (ITPro, 2024). Threat actors include nation states, criminal organizations, hacktivists, highly skilled individuals, and rival corporations, who are all additionally augmented by AI. The expansion and widespread adoption of cloud computing, mobile platforms, and interconnected global supply chain networks have vastly increased the attack surface, all while a single weak link within the system can be exploited and used to wreak significant damage in a very short period of time. Because of these challenges, cybersecurity firms must respond faster, analyze far larger data sets, and understand threat behavior at a level that is beginning to elude and exceed normal human capabilities.

FireEye, which following a 2021 restructuring now operates under the name Mandiant, is one of the cybersecurity organizations that are attempting to address these challenges. For clarity, this paper will continue to refer to the firm as FireEye. Founded in 2004, FireEye established its reputation by using virtual machine sensors, advanced detection tools, and human driven intelligence analysis to identify and stop sophisticated malware (FireEye, 2019a). FireEye provides email, network, and endpoint security to more than 9,000 customers across 103 countries and provides support to over 1,000 government and law enforcement agencies around the world. These customers include Visa, Booz Allen, HP, major government ministries, defense agencies, multinational corporations and critical infrastructure operators that all rely on FireEye for guidance, threat intelligence, and active incident response (Enlyft, 2020).

Originally, FireEye utilized virtual machine sensors and human experts to analyze and categorize threats. As threats to cybersecurity evolved, so did FireEye. FireEye transitioned from a hardware-oriented model into a software as a service approach, which allowed it to deliver intelligence to customers faster and on a global scale. FireEye also expanded into

developing cloud-based defenses for its customers and making use of data driven analytics to support decision making and augment the capabilities of human experts (FireEye, 2019a). The company now uses a hub and spoke architecture in which machine generated threat data from email, network, and endpoint sensors is transmitted to a central cloud-based platform where human analysts evaluate, interpret, and act on the results (FireEye, 2019a).

FireEye has deployed over 17 million virtual machine sensors and blocks between 50,000 and 70,000 malicious events every hour, which shows how effective and necessary its architecture model and Human + AI model are for real time detection at a global scale. FireEye also monitors and tracks 40 nation state APT groups, 10 financially motivated groups, and approximately 2,000 newly identified or minor threat clusters (FireEye, 2019b). FireEye's human experts reverse engineer malware, attribute responsibility for attacks, and provide guidance to public and private organizations during and after major incidents (FireEye, 2019a).

FireEye developed their Human + AI strategy because modern cyberthreats have reached a level where human analysts alone cannot analyze the vast volumes of data, logs, telemetry, and other indicators fast enough to respond in a manner that would prevent catastrophic or major damage. AI tools are able to process large data sets and identify statistical patterns, anomalies, and similarities to other threats at speeds that humans cannot match. However, humans provide contextual intelligence, conduct further investigation, use logic, creativity, and strategic judgement, and provide a final level of accountability in the decision-making process which AI cannot replace. The success of this hybrid model was demonstrated when FireEye's machine-learning–driven product, MalwareGuard, won the U.S. Navy's prestigious AI ATAC competition for its ability to detect advanced malware using ML models trained on FireEye's global threat telemetry (Business Wire, 2020)

Despite this advanced and proven model, no system is perfect, and threats continue to evolve. In December 2020, FireEye disclosed that it had been breached by a highly sophisticated nation state actor that stole proprietary red team tools used for penetration testing. According to Reuters, this attack was significant because FireEye is a leading cybersecurity firm and their reputation is built on identifying and preventing cyberattacks. Additionally, the intruders were able to succeed through the use of custom engineered malware and zero-day vulnerabilities

that bypassed advanced monitoring and detection systems (Reuters, 2020). This breach shows that even with extensive, proven intelligence networks and a Human + AI model, any organization is still vulnerable to highly advanced attackers, which with the rise in generative AI, may become more common. Additionally, the theft of the red team penetration testing tools could be used to develop or enhance future malware (Twingate, 2020).

FireEye's ability to remain a leader in cybersecurity depends on continuous innovation in both AI technologies and human expertise. The Human + AI model is necessary because modern cyberattacks occur at speeds and scales that require automation and human judgment to work together. The 2020 breach demonstrates that this model is not foolproof, and future success will require ongoing refinement, improvement, and adaptation.

Cybersecurity is moving toward a future where human judgment and machine intelligence must work together at all times, because neither alone is sufficient to counter threats that continue to grow in speed, automation, and complexity.

What kind of projects are more suitable for AI implementation? Why? (Huy, Michael)

The projects that are most suitable for AI implementation are high volume, repetitive, and pattern-based tasks that have access to reliable and high-quality data. These are the projects where humans struggle because of scale and fatigue, which increase the likelihood of human error rather than reflect a lack of capability. In contrast, tasks that demand contextual understanding, interpretation of intent or mitigating circumstances, negotiation, and creative problem solving are most suitable for human experts.

FireEye makes use of an automatability spectrum to evaluate projects for automation. On one end of the automatability spectrum are tasks that are highly automatable: projects like large scale pattern matching, anomaly detection, similarity comparisons, and automatic triage (Wright, 2019). On the other end of the automatability spectrum are tasks that require strategic judgement and contextual reasoning, projects suited for humans to take care of.

One example of a task that was highly suitable for AI at FireEye was comparing malware and threat artifacts to existing clusters and data to determine attribution and similarity. This type of task is well suited for automation because FireEye has access to huge volumes of data

and historical telemetry, and because it would take far longer for a human to do the brute work (Berninger, 2019). FireEye developed the Atomicity similarity deducing algorithm in order to automate this task. Atomicity helps the human analysts track, group, and analyze threats against existing data by generating similarity matches.

FireEye has deployed over 17 million virtual machine sensors and blocks between 50,000 and 70,000 malicious events per hour, which requires collection, filtering, organization, and analysis to be operationally manageable (FireEye, 2019a). This is another example of a project that is highly suitable to be automated. FireEye developed the Helix platform, which collects machine-generated signal data from email, network, and endpoint sensors and centralizes it for automated correlation and prioritization. This task is well suited for AI because it involves standardizable data inputs and high event volumes, which Helix can process far faster than a human analyst could (Stone, 2019).

AI is more suitable for these projects because the models have sufficient historical data to train on and the environment is stable enough for the patterns observed in the past to remain useful and indicative of current threats. Automating these projects also provides cost-value benefits. A human expert manually reviewing telemetry, malware samples, and millions of logs would require a lot of time and labor; not only taking longer but costing more the longer it takes. An AI model reduces the workload drastically, and in the long run the cost is ultimately less. Additionally, in projects like these, human analysts still validate and interpret the findings of the AI and apply human judgement and knowledge, which can mitigate any errors or hallucinations the AI might have.

Projects that require strategic judgement, contextual reasoning, and interpretation of circumstances and intent are far less suitable for AI implementation. Humans excel at interpreting context, handling novel situations with little prior data, and reasoning under ambiguity, while AI models are limited to the data they were trained on and the specific tasks they were designed to perform. Determining whether a series of cyber intrusions should be attributed to a specific APT group, what their objectives are, and how an organization should respond requires expertise that goes beyond pattern recognition. These tasks require human

threat analysts to interpret intelligence across multiple sources and contexts, a process supported and augmented, but not replaced by AI (FireEye, 2019a; Bricata, 2019).

Even when a project appears suitable for automation, its success depends on critical parameters such as whether the model can adapt to changing data, whether it can be effectively incorporated into existing workflows, and whether the organization is prepared to adopt and use the system correctly (Wright, 2019). The AI must be tailored to handle the specific project, even if the project is suited for AI automation.

AI provides speed, scale, and consistency, and humans provide contextual understanding, ethical judgment, and strategic direction. In summary, the projects most suitable for AI at FireEye are those where machines can take over the heavy lifting of data processing and pattern recognition, while human experts retain control over interpretation, escalation, and decision-making.

What was FireEye's AI strategy? (Huy)

FireEye's AI strategy was built around augmentation rather than replacement. FireEye's objective was to use AI and machine learning to multiply the power, reach, and speed of human analysts. FireEye views AI as a way to reduce the volume of repetitive analytical work, accelerate detection, and give analysts the time and intelligence needed to make decisions (Wright, 2019).

A central part of FireEye's AI strategy was the use of the automatability spectrum, which provided a framework for deciding which tasks and projects could be delegated to AI and which required human expertise. Tasks on the highly automatable end of the spectrum include large scale pattern matching, similarity comparisons, anomaly detection, clustering, and automated triage, all of which are projects where AI can operate reliably when given large and consistent datasets (Wright, 2019). Tasks that fall on the human oriented end of the spectrum include analysis of novel attacks, interpretation of context, assessment of attacker intent, and decision making. FireEye's AI strategy depended on assigning the right tasks suited to the strengths of humans or machines

FireEye implemented this strategy through a human-machine ecosystem built around the cloud platform Helix. Helix acted as the operational layer for the strategy, collecting vast amounts of machine generated telemetry from FireEye's email, network, and endpoint sensors and centralizing it for automated scoring, filtering, and correlation (Stone, 2019). With over 17 million virtual machine sensors deployed around the world, and blocking tens of thousands of malicious events every hour, FireEye needed an automated system that could handle the scale and volume of data and present analysts with prioritized outputs rather than raw, unfiltered data (FireEye, 2019a). Helix integrated machine generated threat data, analytics tools, and incident response capabilities into a seamless ecosystem that reduced response times for human experts processing and acting on data.

In addition to Helix, FireEye developed several other specialized AI models and algorithms as part of its automation strategy. The Atomicity similarity deducing algorithm was built to automate the work of comparing new malware samples and threat artifacts to historical and existing clusters across multiple dimensions (Berninger, 2019). Atomicity handled the heavy lifting in identifying potential similarity matches, and analysts reviewed the results and interpreted them within the context of the broader threat landscape (Miller & Davenport, 2020). FireEye also used MalwareGuard, a machine learning based detection engine trained on global telemetry, which demonstrated the effectiveness of this hybrid strategy by winning the U.S. Navy's AI ATAC competition for detecting advanced malware (Business Wire, 2020).

Another major aspect of FireEye's AI strategy was ensuring organization readiness, training, and proper integration of AI models and algorithms into the existing workflows. Successful creation and use of AI requires that threat analysts, data scientists, and IT engineers work together during model development, testing, and deployment (Oracle & KPMG, 2019). Additionally, FireEye encouraged their analysts to question AI outputs, flag, and provide feedback on incorrect predictions for retraining, reducing the risk of blind trust, and overreliance on automated results (Bricata, 2019). This ensured that AI models were accurate and regularly updated, and that analysts understood how to use the outputs correctly, and knowledgeably.

Overall, FireEye's AI strategy aimed to build a scalable and adaptive system that could respond to quickly evolving threats across multiple industries and countries. FireEye created a strategy that could detect, classify, and respond to threats faster than either AI or humans could alone, by combining the scale and computational power of AI with the judgement and logic of human experts.

Why did FireEye opt for the Human + AI approach? What are the benefits and advantages of such an approach? What are the limitations and disadvantages of such an approach? (Jorge)

There are significant benefits to the Human + AI strategy beyond pure, competitive necessity. The approach reduces the analyst workload by automating the most repetitive and time-consuming tasks, in turn increasing efficiency, decreasing response times and strengthening the overall resilience of FireEye's systems, and services. It improves accuracy by allowing machine learning models to detect statistical anomalies and identify patterns that humans may overlook when fatigued. The strategy also increases scalability because AI can process the incoming data at speeds humans cannot, and adding more sensors and telemetry would not slow the models like it would slow down human teams. There are also inherent cost-value benefits that come from the use of AI models and algorithms, since automation reduces the labor hours required for brute-force analysis and allows highly trained analysts to focus their time on complex decision making and investigative tasks. Finally, the combination of AI and human expertise creates a feedback loop: analysts validate model outputs and report inaccuracies, which allows the data science teams to retrain the models and improve performance over time (Oracle & KPMG, 2019; Bricata, 2019). MalwareGuard, which won the U.S. Navy's AI ATAC competition, showed how AI trained with FireEye's global telemetry could detect advanced malware more effectively than traditional signature-based approaches (Business Wire, 2020).

However, there are some disadvantages and limitations in the Human + AI strategy. AI systems heavily rely on having large quantities of vetted, high-quality data. This raises the barrier for entry; other organizations might struggle to implement a similar strategy because they do not have access to the huge volumes of historical data FireEye has. Additionally, unseen

or novel malware can bypass AI detection and identification systems because the models have no prior examples in their training to draw on. AI systems can generate incomplete or misleading outputs if their training data is skewed, poisoned, incomplete, irrelevant, or outdated, which can make the model a liability Additionally, AI systems can generate incorrect or misleading outputs if the underlying training data is skewed, if adversaries intentionally poison data sources, or if the model has not been recently retrained to reflect newly observed threat behavior (Wright, 2019). With the rise in generative AI, attackers can make use of machine learning techniques and AI tools to refine their malware and capabilities, and automate large scale attacks.

FireEye chose the Human + AI strategy because it allowed the firm to use automation where it is most effective, and human expertise where judgement and decision making are required. The approach provides speed, scale, and analytical capabilities that exceeds what mere mortals may be capable of, while still retaining the logic, ethics, and accountability that AI cannot replace. However, no system is perfect and there are real limitations, which are primarily the necessity for a high volume of high quality, reliable data, and the inability of AI detection systems to properly detect novel and unknown threats. The Human + AI model is not a foolproof defense, but rather a necessary and adaptive strategy that allows human experts to compete with the speed, complexity, and continuous evolution of modern cyberattacks.

What are the key parameters for successful AI implementation in an organization? How did FireEye ensure that employees in its organization could adapt to the AI mindset? (Abdullah)

Successful AI implementation in organizations depends on several key parameters which decide whether AI systems improve operational efficiency or create additional operational difficulties. The operational environment of FireEye shows how these parameters affect mission success through their impact on speed, accuracy, and analyst workload. The primary parameter for successful implementation of AI in an organization is access to large amounts of high-quality information. AI models need structured reliable data for both training, and the tasks that it automates, such as detecting patterns and similarities. The company achieved success with its AI tools because it gathered telemetry data from 17 million sensors which tracked customer

network activity. The models at Atomicity and MalwareGuard learned from extensive real-world data because they received continuous threat indicators and malware samples and behavioral patterns (FireEye, 2019a; Berninger, 2019). Pattern matching and anomaly detection tools need large amounts of data to operate at high speeds and generate precise predictions which support real-time defense operations.

The second parameter is proper integration into an organization's workflow. AI systems need to be embedded into operational systems and processes in a transparent and non-disruptive manner. The Helix platform from FireEye serves as the main system which centralized all the incoming telemetry data, runs triage, clustering and correlation functions to curate prioritized cases for human analysts to review before taking action (Stone, 2019). The system eliminated unnecessary information while eliminating repetitive work and stopping analysts from spending time on unimportant tasks. AI systems improved operational efficiency through their workflow assistance which operated as non-intrusive tools for analysts.

Not only does the AI need to be properly embedded within the organization’s workflow and systems, but the organizations and analysts themselves need to be prepared and ready to adopt and make use of AI. Organizational readiness is a key parameter which determines success in implementing AI. Staff members need to understand AI system operations and learn how to evaluate system results and when to verify system outputs that appear incorrect. FireEye did this through employee training sessions which focused on teaching analysts how the models made predictions, how to recognize correct outputs, and how and when to challenge and override the AI systems. These processes prevented blind trust in automation and created a continuous improvement cycle, where analysts helped refine and retrain models over time (Bricata, 2019; Oracle & KPMG, 2019). This approach also reinforced the principle that AI assists with heavy data processing, but human experts must retain ultimate decision authority.

The fourth essential parameter for successful AI implementation depends on cross functional collaboration between different teams. AI implementation fails when data scientists operate independently from cybersecurity analysts and engineers. FireEye prevented this failure by making analysts and engineers active participants in AI system development and

testing and optimization processes. The analysts brought operational knowledge and experience to help explain attacker actions while selecting the key elements they needed for attribution and clustering tasks. This collaboration ensured that AI tools aligned with real-world requirements and needs, and produced outputs analysts could trust (Wright, 2019).

A fifth parameter is cultural alignment around the Human + AI model, which FireEye reinforced through the use of its automatability spectrum. The automatability spectrum framework helped FireEye define what tasks were appropriate for AI to take over, and which required human judgement. Tasks on the automatable end of the spectrum like pattern matching, similarity scoring, and sensor telemetry filtering were assigned to AI systems like Atomicity, Helix, and machine learning based triage engines. These processes are high volume, highly repetitive that machines can perform faster and more consistently, freeing up time for human analysts to focus on their tasks. The analysis team maintained responsibility for tasks that needed human judgment to understand context and attacker intentions and make strategic decisions (Miller & Davenport, 2020). By using the automatability spectrum to clearly outline the rules and responsibilities for AI implementation, FireEye reduced staff tension and resistance, increased acceptance of AI tools, and created shared expectations about the purposes and limits of the AI systems.

Another essential factor is the need for regular retraining and maintenance of the AI tools. According to FireEye, “ML models experience an inherent struggle: not retraining means being vulnerable to new classes of threats, while retraining causes churn and potentially reintroduces old vulnerabilities” (FireEye, 2019c). For successful implementation of AI systems, organizations need to plan for regular retraining and validation cycles, monitoring frameworks to prevent model drift, and have contingency plans in place.

FireEye established an operational framework which enabled AI systems to work alongside and enhance human experts through these defined parameters. FireEye developed dependable data transmission systems which merged equipment with operational processes and provided training to analysts and fostered teamwork and developed an organizational environment that viewed AI technology as an improvement tool. FireEye ensured that their analysts adapted successfully to an AI augmented environment while maintaining human

judgement as the foundation of their cybersecurity operations, even as their operations went global.

Conclusion (Jorge)

The rise of AI enabled support systems and automation is part of the long historical pattern in which organizations adopt increasingly capable technologies to manage scale and improve efficiency. FireEye's own development reflects this evolution. The firm originally operated as a hardware-oriented provider built around virtual machine sensors, however over the years they transitioned into a software as a service-based organization in order to handle the newfound demands for speed and volumes of data being analyzed (FireEye, 2019a). The Human + AI model is the next step in that progression.

Previously, AI only existed in very simple, rule-based forms that executed fixed logic rather than adapting to new threats and learning from data. In the 1980s, AI existed but functioned like traditional automation. The introduction of machine learning changed this; rather than following predetermined instructions, ML-based systems can learn from data, identify patterns, and generate predictions that were not specifically programmed into it. By 2019, 53% of organizations surveyed in the cybersecurity sector have incorporated machine learning systems into their security workflow, which shows that FireEye's development was a part of a greater industry shift into making use of a new, adaptive technology (Oracle & KPMG, 2019).

FireEye processes data from over 17 million virtual machine sensors and blocks tens of thousands of malicious events every hour, tasks no human team or regular hardware could stay on top of (FireEye, 2019b). The use of AI systems like Helix and Atomicity are crucial and allow FireEye to automate triages, clustering, anomaly detection, and similarity match so that human analysts can focus on oversight, real-world interpretations, and decision making (Berninger, 2019; Stone, 2019). Rather than replacement, this upgrades human capabilities by managing the scale of the data.

The growth in cybersecurity spending from $43.1 billion in 2020 to $213 billion in 2025 shows how necessary cybersecurity has become, and the demand for the next step in cyber-

defense (Statista, 2020; ITPro, 2024). Firms like FireEye are a huge part of that expenditure, and they have developed their Human + AI strategy in a way that it is scalable and can adapt to the threat environment as it evolves.

This isn't entirely uncharted waters for organizations either. Federal cybersecurity frameworks provide guidance and structures that integrate with AI processes, allowing for organizations to begin transitioning into Human + AI strategies themselves. Under the NIST SP 800 37 Risk Management Framework, AI enabled monitoring fits naturally within the Continuous Monitoring step, where automated mechanisms support ongoing authorization decisions by collecting, correlating, and flagging relevant security data for analysis and evaluation by a human official (National Institute of Standards and Technology, 2018). Similarly, under NIST SP 800 53, AI tools can enhance controls like AU-6 (Audit Review), which requires timely analysis of audit records, by automatically identifying anomalies for human review. AI can also enhance controls like IR-4 (Incident Handling), which explicitly calls for automated mechanisms to support detection, analysis and prioritization (National Institute of Standards and Technology, 2020). These frameworks already assume the need for automation and human oversight working together, which means organizations are able to adapt to the changes and necessity of Human + AI strategies going forward.

The shift from rule-based automation to adaptive machine learning based automation introduces a new challenge; that organizations and the humans that use the systems must determine when to trust the output of the AI model, and when to apply human judgement. Because there is a continuous concern about whether the output of an AI is reliable, human oversight is always necessary. FireEye's own process reinforces this; their analysts must continuously review the AI outputs, report and correct errors, and regularly refine and retrain their models with new data. This feedback loop allows the AI systems to evolve over time and improve in ways that resemble a learning process rather than static automation. Modern machine learning systems function less like a traditional tool and more like a real partner that improves through guidance and experience, almost like a new human analyst learning and improving through mentorship.

AI enabled automation and support systems are a continuation of the existing technological progression, and even a necessary evolution for organizations to survive in the modern cybersecurity landscape. FireEye's Human + AI model shows that speed, scale, and analytical capability must be paired with human judgment, ethical reasoning, creativity, and accountability. While modern AI introduces new uncertainties, it also integrates cleanly into existing cybersecurity frameworks such as NIST SP 800-37 and NIST SP 800-53, which already emphasize continuous monitoring, automated mechanisms, and human oversight. The primary concern in the adoption of these strategies is carefully integrating AI processes into existing workflows, because poorly trained AI or integration without training could result in greater impact to a system than a cyberattack.

References

Berninger, M. (2019, March 26). *Going Atomic: Clustering and associating attacker activity at scale.* Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/clustering-and-associating-attacker-activity-at-scale/

Bricata. (2019). *Signature detection vs. network behavior.*

Business Wire. (2020, March 4). *NAVWAR enterprise awards FireEye first place in Artificial Intelligence challenge* [Press release]. https://www.businesswire.com/news/home/20200304005014/en/NAVWAR-Enterprise-Awards-FireEye-First-Place-in-Artificial-Intelligence-Challenge

Enlyft. (2020). *Companies using FireEye.* Enlyft. https://enlyft.com/tech/products/fireeye

FireEye. (2019a). *FireEye annual report 2019.* FireEye, Inc. https://www.annualreports.com/HostedData/AnnualReportArchive/f/NASDAQ_FEYE_2019.pdf

FireEye. (2019b). *M-Trends 2019: FireEye annual threat report.* FireEye, Inc. https://services.google.com/fh/files/misc/m-trends-report-2019-en.pdf

FireEye, Inc. (2019c, April 9). *Churning out machine learning models: Handling changes in model predictions*. https://cloud.google.com/blog/topics/threat-intelligence/churning-out-machine-learning-models-handling-changes-in-model-predictions/

Joint Task Force Transformation Initiative. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

ITPro. (2024, July 30). *Global cybersecurity spending is going to hit $213 billion in 2025 — here's what's driving investment.* https://www.itpro.com/security/global-cybersecurity-spending-is-going-to-hit-usd213-billion-in-2025-heres-whats-driving-investment

Miller, S., & Davenport, T. (2020). *The Future Of Work Now: Cyber Threat Attribution At FireEye.* FireEye. https://www.forbes.com/sites/tomdavenport/2020/05/28/the-future-of-work-now-cyber-threat-attribution-at-fireeye/

National Institute of Standards and Technology. (2020a). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Oracle, & KPMG. (2019). *Oracle and KPMG cloud threat report 2019.* Oracle Corporation. https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf

Reuters. (2020, December 11). *U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools.* Reuters. https://www.reuters.com/business/us-cybersecurity-firm-fireeye-discloses-breach-theft-hacking-tools-2020-12-11/

Statista. (2020). *Spending on cybersecurity worldwide from 2017 to 2020* https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/?srsltid=AfmBOorpYKoKnUYRvoyboARzmisvCfX1GylJF7w8IeA6X8y3cRACVBD9

Stone, S. (2019). *Trends in Big Evil Hunting* [Conference presentation]. FireEye Cyber Defense Summit. https://www.youtube.com/watch?v=B9Z2nv1Wgfo

Twingate. (2020). *FireEye data breach: What happened and what we know.* https://www.twingate.com/blog/tips/FireEye-data-breach

Wright, E. (2019, October 8). *The shifting balance: Expertise, automation, and the future of cybersecurity* [Webcast].

Team Members and Contributions

Group 7 Team Member	**Contribution**
Michael	Summary, Q1, editing, proofreading
Huy	Q1, Q2, research, proofreading
Jorge	Q3, Conclusion, research, editing, proofreading
Abdullah	Introduction, Q4, research, editing, proofreading