

The Role of Proactive Leadership in Cyber Crisis Management: Artificial Intelligence as a Decision-Making Tool (An analytical and descriptive study)

دور القيادة الاستباقية في إدارة الأزمات السيبرانية: الذكاء الاصطناعي
كأداة للقرار الإداري
(دراسة تحليلية وصفية)

Nechadi Abderrahmane

University of Blida2 Lounici Ali

a.nechadi@univ-blida2.dz

Received date: 12 / 10 / 2025

Acceptance date: 09 / 10 / 2025

ملخص:

تتناول هذه الدراسة دور القيادة الاستباقية في تعزيز قدرة المنظمات على مواجهة التهديدات السيبرانية، خاصة عند
توظيف الذكاء الاصطناعي في صنع القرار. وتبين أن القيادة الاستباقية، بخلاف القيادة التفاعلية، تعتمد على
التنبؤ بالمخاطر واتخاذ الإجراءات الوقائية قبل وقوع الأزمات. ويُعد الذكاء الاصطناعي أداة استراتيجية تُمكن من
تحليل البيانات الضخمة، كشف السلوكيات غير الطبيعية، والتنبؤ بالهجمات المحتملة. غير أن فعالية هذه التقنيات
تبقى مرهونة بقدرة القادة على فهمها ودمجها ضمن البنية الأمنية للمؤسسات. وتبرز دراسة حالة هجوم
SolarWinds كيف ساهمت الشفافية، تبادل المعلومات، والاستثمار المبكر في الأنظمة الذكية في الحد من
الأضرار. وتخلص الدراسة إلى أهمية بناء قيادات رقمية، وتعزيز التعاون المؤسسي، مع ضرورة تدريب القادة
ووضع أطر قانونية وأخلاقية لضمان الاستخدام المسؤول للذكاء الاصطناعي في المجال السيبراني.

الكلمات المفتاحية: القيادة الاستباقية، الذكاء الاصطناعي، إدارة الأزمات السيبرانية، داركتراس (Darktrace)،
هجوم سولار ويندز (SolarWinds Attack).

Abstract:

This study highlights that proactive leadership represents the key factor in enhancing organizations' ability to confront cyber threats, particularly when integrated with artificial intelligence (AI) mechanisms. Unlike reactive leadership, which is limited to responding after an incident occurs, proactive leadership focuses on risk anticipation, preventive initiatives, and advance preparedness, enabling intervention before a breach escalates. In this context, artificial intelligence is an essential strategic tool capable of analyzing vast amounts of data, detecting anomalous behaviors, and predicting potential attacks, as demonstrated by systems such as Microsoft Defender, Azure Sentinel, and Darktrace. However, the effectiveness of these tools critically depends on the presence of leaders who understand their capabilities and can make

strategic decisions to integrate them into the organization's security framework. The real-world case of Microsoft's response to the SolarWinds attack illustrates how transparency, information sharing, and early investment in intelligent systems contributed to mitigating damages and protecting critical infrastructure. It is from this insight that the importance of developing digital leadership capabilities and strengthening collaboration with external stakeholders emerges. The study recommends the necessity of training leaders in technical aspects, investing resources in early detection systems, and establishing legal and ethical frameworks to ensure responsible and transparent use of artificial intelligence in the field of cybersecurity.

Key words: Proactive Leadership, Artificial Intelligence, Cyber Crisis Management, Darktrace, SolarWinds Attack.

Introduction:

As digital transformation accelerates in today's world, we are also seeing a corresponding rise in sophisticated cyber risks. In the dynamic environment of this tremendous growth in areas of rapid digital acceleration, governments, organisations and companies face unprecedented challenges in protecting their business data and IT infrastructure. Attacks are no longer considered purely technical risks; they have become strategic threats to a company's survival, financial stability, and reputation. As cyber threats increase, so does the need for a new type of leadership capable of thinking and acting quickly before a crisis, known as 'proactive leadership' rather than the usual reactive approach, which focuses on responding after a breach, while the proactive approach focuses on prediction, protection, and preparation.

There is also cause for concern regarding the increasing severity of challenges organisations face in managing these crises. As indicated in the latest reports issued by ISC2 in 2024, there is an estimated shortage of 4.7 million cybersecurity professionals worldwide. (ISC2, 2024) This gap in human expertise and skills has prompted organisations to adopt artificial intelligence mechanisms as an essential part of proactive leadership.

There is no doubt that the nature of cyber threats has shifted from simple individual attacks to highly sophisticated operations, often organised and supported by states or criminal groups. Modern threats therefore require new defensive measures combined with modern technologies that make the defence process more proactive. In this regard, artificial intelligence has become an important tool in improving defensive capabilities, as it can analyze vast amounts of data to detect potential threats in real time. However, the effectiveness of these technologies remains dependent on rapid response through proactive leadership capable of directing the technologies appropriately.

From this perspective, the fundamental problem of this research emerged: many institutions are no longer keeping pace with these rapid developments and, consequently, remain vulnerable to surprise cyber attacks. This is especially true in a world that is becoming more complex by the day, where traditional leadership is no

longer sufficient. Focusing on proactive leaders who use artificial intelligence for prevention and detection has become essential for ensuring the continuity and safety of organisations in today's cyber space. In this context, this research explores how organisations can employ proactive leadership — a critical competence in crisis management — and its pivotal role in addressing cyber challenges.

This study is significant because it combines three fields of knowledge: administrative leadership, cybersecurity, and artificial intelligence technologies. It also contributes to filling an important research gap related to the mechanisms of integrating modern technologies into cyber crisis management strategies. Additionally, it provides an analytical framework for successful practices in organisations, thus representing an important investment in their digital future. Leadership today is no longer limited to decision-making, but extends to building a secure and resilient digital ecosystem. Therefore, understanding the relationship between proactive leadership and artificial intelligence mechanisms is a crucial step towards building more secure and adaptable organisations in cyberspace.

This study will discuss the theoretical framework of proactive leadership, cyber crisis classifications, and artificial intelligence tools used for this purpose, including IBM QRadar Suite, Darktrace, Azure Sentinel, and other intelligent applications. This will be followed by an analysis of real-world case studies, such as Microsoft's response to the SolarWinds attack, and finally, practical recommendations for practitioners and decision-makers.

In the era of digital transformation, cyber crises have become an increasingly significant threat affecting businesses and governments alike. Organizations face significant challenges in keeping up with the evolving methods of cyberattacks, which are characterized by complexity and organization. While artificial intelligence technologies offer promising solutions for early threat detection, their effectiveness remains dependent on the efficiency of management leadership in deploying them. Many organizations suffer from a clear gap between the available technical capabilities and the ability to strategically utilize them. This issue is exacerbated by the absence of proactive vision and effective leadership frameworks. In this context, a central question arises:

What are the roles of proactive leadership in effectively employing artificial intelligence mechanisms to enhance the capabilities of managing cyber crises within organizations?

Study Questions:

From this problem, the following questions branch out:

- 1- How does artificial intelligence contribute to improving decision-making during cyber crises?

- 2- What types of cyber crises are most responsive to artificial intelligence applications?
- 3- What is the appropriate balance between artificial intelligence and human leadership in cyber crisis management?
- 4- What are the criteria for selecting appropriate artificial intelligence tools to support proactive leadership?
- 5- How do successful institutions like Microsoft apply this integrative model?

Importance of the Study:

Studying this issue holds great importance on academic, practical, and strategic levels, due to the radical changes in the nature of cyber threats, the reliance of modern institutions on technology, and the necessity of intelligent interaction with digital risks. The study's importance can be examined from several key perspectives:

- Confronting increasingly complex cyber threats, exemplified by incidents such as **SolarWinds**
- Integrating artificial intelligence mechanisms into proactive leadership
- Enhancing the ability to manage crises proactively rather than reactively
- Bridging the gap between technology and managerial leadership
- Enriching academic literature in proactive management and technology

Methodology:

This study relied on descriptive analysis of a case study showing how institutions respond to cyber crises.

Limitations of the methodology:

- Reliance primarily on previously published data.
- Difficulty accessing some confidential data.
- Limiting the analysis to the period 2020 and beyond.

Study objectives:

- To demonstrate the possibility of observing and evaluating proactivity in leaders differently by evaluators in different positions.
- To provide a general conceptual analysis of proactive leadership.
- The possibility of subjecting such studies to empirical research.

1. Basic Concepts of the Study

1.1 Proactive Leadership: Definition and Dimensions

Proactive leadership is a forward-looking management approach in which leaders anticipate challenges, take initiative, and implement strategies to prevent problems before they occur. (AURORA, 2025) Scholars define it as generating and implementing self-initiated, future-focused, and sustainable leadership actions to bring

about change. (Wu & Wang, 2011) This strategic management model is characterized by proactive decision-making and preventive action, where leaders systematically identify potential challenges and opportunities to formulate solutions before crises emerge. (Crant, 2000)

1.1.1 Definition Adopted in This Study

Proactive leadership is a leadership style that anticipates future challenges and takes preventive measures before they escalate, rather than simply responding to events after they occur. This leadership style is characterised by three core dimensions:

1. Foresight and prediction: Leaders analyze trends and identify potential risks before they materialize.
2. Initiative-taking: Leaders make proactive decisions based on data and evidence.
3. Flexibility: Leaders adapt strategies dynamically before crises escalate.

1.1.2 Elements of Proactive Leadership

1. Proactive Behavior: Taking initiative and acting preventively before crises occur, rather than reacting after problems emerge.
2. Predictive Analytics: The use of data-driven tools to anticipate risks and opportunities. This includes predictive AI technologies that employ historical data, statistical algorithms, and machine learning to forecast future outcomes. These techniques enable organizations to identify emerging threats and seize strategic opportunities early. (Stryker, 2024)
3. Strategic Adaptation: The organizational capacity to modify core strategies and internal processes in response to environmental changes. This reflects operational flexibility that allows leaders to adjust course based on evolving market conditions and emerging risks.

1.1.3 Characteristics of Proactive Leadership

Proactive leadership is not merely individual behavior, but rather an organized leadership model based on prediction, initiative, and strategic thinking that aims to direct the organization towards the future rather than waiting for crises to occur. It differs from reactive leadership across three key criteria:

1. Timing: Proactive leadership acts before crises emerge, while reactive leadership responds after crises occur.
2. Tools: Proactive leadership relies on artificial intelligence and predictive analytics, while reactive leadership depends primarily on past experience and established protocols.
3. Outcomes: Proactive leadership minimizes potential losses through early intervention, while reactive leadership often faces higher costs associated with crisis response and recovery.

1.1.4 Dimensions of Proactive Leadership

Proactive leadership enhances cost-effectiveness, reduces crisis impact, and fosters strategic thinking that contributes to organizational safety and optimal outcomes. The key dimensions supported by management theories can be summarized as follows:

1. **Foresight:** The ability to anticipate future challenges using tools such as scenario analysis and strategic planning. Example: Microsoft's proactive approach to complex cyberattacks exemplifies practical strategic foresight. Recognizing the evolving threat landscape, Microsoft employs advanced technologies, including artificial intelligence, to detect early indicators of cyber threats. (Schoemaker, 1995)
2. **Initiative-Taking:** Acting proactively to address potential issues before being prompted or required to do so.
3. **Strategic Thinking:** Connecting present actions with future organizational goals and anticipated challenges. (Hax & Majluf, 1991)
4. **Crisis Preparedness:** Developing contingency plans, establishing early warning systems, and conducting regular drills to ensure readiness. (Boin & 't Hart, 2003)
5. **Transparency and Early Communication:** Disclosing risks and threats promptly to relevant stakeholders to enable timely response.
6. **Continuous Learning and Adaptability:** Systematically reviewing performance after each incident to drive ongoing improvement and refinement of strategies.
7. **Shared Responsibility:** Fostering a culture where team members actively participate in threat prevention and organizational resilience.

1.2 Definition of Cyber Crisis

A cyber crisis is defined as a critical situation resulting from a successful cyberattack. These attacks aim to undermine the security of data, infrastructure, and computer systems, and often manifest in major incidents such as ransomware attacks, data breaches, and phishing schemes, posing a threat to organizational continuity. (Arnaud, 2022)

Crises in the traditional sense are events that threaten fundamental values or life-supporting systems and require urgent responses under conditions of deep uncertainty. (Backman, 2020) Building on this understanding, cyber crises are emergency situations resulting from serious cyberattacks or security breaches that threaten information security, disrupt vital processes, or cause significant material or reputational damage to individuals, organizations, or nations. These situations demand exceptional management responses due to their urgency, complexity, and potential for cascading impacts.

1.2.1 Classification of Cyber Threats: ENISA Framework

The European Union Agency for Cybersecurity (ENISA), established in 2004, publishes the annual ENISA Threat Landscape (ETL) report to assess cybersecurity risks across Europe. The 2023 and 2024 editions provide critical insights into the evolving threat environment and serve as authoritative references for understanding current cybersecurity challenges within the European Union.

The report provides valuable insights regarding emerging cybersecurity threats, threat actor activities (especially in the context of ongoing regional conflicts), vulnerabilities, and security incidents. The ETL report aims to guide decision-making, prioritization, and recommendations in cybersecurity policy. It identifies key threats and their characteristics, threat actor motivations, attack methodologies, and provides sector-specific analysis with impact assessments. This analysis is supported by ENISA's Cyber Threat Landscape (CTL) Working Group.

The main threats identified and analyzed in the 2023-2024 reports include:

- Ransomware: Accounting for more than 66% of all reported incidents in October 2023, ransomware remains the dominant threat. (Threat Hunter Team, 2024)
- Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to systems
- Social Engineering: Manipulation tactics targeting human psychology to breach security
- Threats Against Data: Unauthorized access, theft, or exposure of sensitive information
- Threats Against Availability (Denial of Service): Attacks designed to disrupt or disable services and infrastructure
- Information Manipulation and Interference: Disinformation campaigns and content manipulation
- Supply Chain Attacks: Compromising trusted third-party vendors or software to infiltrate target organizations(ENISA, 2023)

The report is complemented by a detailed analysis of the vulnerability landscape during 2023 and 2024, as well as an in-depth examination of four categories of threat actors:

- State-Nexus Actors: Threat actors with links to or support from nation-states
- Cybercrime and Hacker-for-Hire Actors: Criminal groups and mercenary hackers operating for financial gain
- Private Sector Offensive Actors (PSOA): Commercial entities providing offensive cyber capabilities and surveillance tools
- Hacktivists: Ideologically or politically motivated actors conducting cyber operations to promote specific causes(Chandola et al., 2009)

The ETL 2023 report showed that public administration as the most targeted sector by about 19%, followed by targeted individuals (about 11%), then Health (about 8%), digital infrastructure (about 7%), then manufacturing, finance and transport sectors. (IBM, 2025)

2. Artificial Intelligence in Decision-Making: Tools and Applications in Cyber Crisis Management

2.1 Machine Learning to Detect Abnormal Patterns

This action refers to the identification of anomalies, which are patterns in data that deviate from expected behavior. Such non-conforming patterns are often called anomalies, outliers, exceptions, or deviations. In the context of anomaly detection, "anomalies" and "outliers" are commonly used interchangeably. Anomaly detection is widely applied in various fields, including credit card, insurance, and healthcare fraud detection, as well as intrusion detection in cybersecurity, fault detection in critical safety systems, and military surveillance of enemy activities. (Darktrace, 2025)

Accordingly, machine learning for detecting abnormal patterns (Anomaly Detection using ML) is a branch of artificial intelligence used to identify data points or events that significantly deviate from expected behavior in a dataset. This is achieved using statistical models or machine learning algorithms such as Random Forest and LSTM Networks, which are effective for detecting time sequences of extended attacks.

One notable application is IBM QRadar, which analyzes network flows to proactively detect attacks. The company offers an updated and always-connected security software suite called IBM QRadar Suite. This suite is designed to help security teams manage and respond to incidents more efficiently, supporting enterprise-wide processes and enhancing organizational security through core technologies. (Darktrace, 2017)

2.2 Darktrace Systems for Automatic Detection of Attacks

Darktrace systems utilize adaptive artificial intelligence in cybersecurity to analyze the behavior of networks, users, and devices. They create a "physiological picture" of the network, known as Cyber DNA, which reflects the natural patterns of behavior. When any abnormal behavior is detected—such as unusual connections or the transfer of large amounts of data—the system triggers an immediate alert.

The Darktrace ActiveAI security platform is built on industry-leading artificial intelligence that learns the typical behavior of an organization. This enables it to proactively detect and stop both known and new threats. (Recorded Future, 2025) For example, the WannaCry malware attack is unprecedented in scale, affecting more than 200,000 devices in 150 countries, according to Europol, and demonstrating how Darktrace systems were used to monitor the threat within minutes. Nicole Egan, CEO

of the company, says: "The WannaCry virus has bypassed traditional security defenses, proving useless in the new era of cyber warfare. Security teams cannot meet this challenge without having the right tools. The Darktrace Enterprise Immune System is a real example of artificial intelligence at work: detecting and stopping threats before they are noticed by human teams." (Shain, 2020)

In addition to these mechanisms, Microsoft considers it necessary to train employees regularly, conduct penetration tests, and improve user behavior to reduce cyber risks. The result is a prevention of its spread to 90% of network devices. (U.S. GAO, 2022)

Natural Language Processing (NLP) is used for threat analysis, particularly in monitoring communication platforms to detect hate speech that may precede political cyber attacks. The Recorded Future platform is one of the largest platforms dedicated to identifying critical threats, helping organizations prioritize and act quickly before attacks can form and disrupt operations. (Clayton, 2025)

3. Analysis and Discussion

3.1 Case Study of the SolarWinds Attack (2020)

At the end of 2020, an advanced and complex cyber attack was revealed, targeting numerous government and commercial organizations worldwide. This included the US Treasury Department, the Department of Homeland Security, major technology companies, and other vital institutions. The SolarWinds, also known as the Solorigate or Sunburst attack, (Jones, 2025) is a prominent cybersecurity incident that significantly affected the US government.

The Russian Foreign Intelligence Service hacked the SolarWinds Network Management Program, which is widely used in the US government. Additionally, there are indications that Chinese government entities exploited a security vulnerability in the Microsoft Exchange Server. (Microsoft, 2025) This vulnerability was leveraged by injecting the Sunburst virus via the SolarWinds Orion software update. As a result, devices became open to attackers, allowing them to spy, steal data, and navigate within the network.

3.2 Case Analysis of Microsoft's Response to the SolarWinds Attack (2020)

3.2.1 Proactive Leadership Roles:

3.2.2 Quick Diagnosis

Although Microsoft was not the initial primary target, it was one of the most important victims and secondary targets, as the attackers used Microsoft tools (such as Azure, Outlook, and Exchange) to expand the scope of the attack. However, the company demonstrated a quick and proactive response that serves as a global model in cyber crisis management.

Azure Sentinel tools, powered by artificial intelligence, were used to detect abnormal patterns in data traffic within 40 minutes of the attack starting. Azure Sentinel simplifies the process of collecting data from multiple sources across different environments, both on-premises and in the cloud. This enables the detection of attacker activities (known as Tactics, Techniques, and Procedures, or TTPs) in data that is available by default or can be integrated into Azure Sentinel. (Shain, 2020)

3.2.3 Proactive Decision Making and Strategic Communication

Microsoft was one of the first companies to publicly announce the SolarWinds attack, even before many government agencies fully realized the severity of the situation. The following actions were taken:

- Formation of a Special Response Team: A dedicated team with non-bureaucratic powers was established, headed by the Vice President for Cybersecurity.
- Immediate Decision: All SolarWinds updates were disabled, despite the associated operational costs.
- Transparent Reporting: Within 24 hours, transparent reports were issued to agencies such as the FBI, CISA, and the US Congress.
- Collaboration with Security Companies: Microsoft collaborated with security firms like CrowdStrike and FireEye to share critical data.
- Immediate Reporting to Authorities: The company promptly reported to authorities and the international community to warn them of the threat and prevent its wider spread.
- Information Sharing: Information was shared with both the private and public sectors to enhance collective security efforts. (Clayton, 2025)

Microsoft's Proactive Response to the SolarWinds Attack

The SolarWinds 2020 attack, considered one of the most sophisticated and destructive cyber attacks in modern history, revealed that Microsoft was one of the few entities to take a series of proactive and responsible measures. This response has become a role model in the field of cybersecurity. Although the company was among the victims, it quickly transitioned from a position of defense to one of leadership, aiming not only to protect itself but also to safeguard the entire global digital ecosystem by:

1. Early Detection Using Artificial Intelligence

Microsoft relied on advanced artificial intelligence systems, such as Microsoft Defender for Identity and Azure Sentinel, to detect subtle changes in network behavior. These systems can distinguish abnormal behavior even when it is not associated with known malware. Thanks to this intelligent model, the company monitored suspicious activity within its internal network before attackers could access sensitive data or

expand their penetration. Microsoft later confirmed that the attack was "limited" and did not affect customer data, thanks to this quick detection.

2. Instant Transparency

The company promptly informed the public, customers, and authorities, which helped warn other enterprises of the imminent danger.

3. Wide Sharing of Information

Microsoft treated the attack as a threat to the global digital infrastructure, publishing detailed technical analyses of the Sunburst malware, including its behavior, connection mechanisms to remote servers, and camouflage methods. It made all penetration indicators available for free via its platforms and collaborated closely with security companies like FireEye and CrowdStrike, (Jones, 2025) as well as government agencies such as CISA and the FBI, to share information and strengthen collective protection.

4. Continuous Improvement and Preventive Innovation

After the attack, Microsoft moved beyond detection and response to future prevention. The company launched automatic security updates across all its products and released its annual Digital Defense Report, which analyzed the attack and provided strategic recommendations to the public and private sectors.

5. Ethical Leadership and Advocacy for International Organizations

A highlight of Microsoft's response is its engagement with the ethical and political dimensions of cybersecurity. The company has repeatedly called for the creation of an international digital treaty to prevent countries from targeting critical infrastructure such as hospitals, energy, and education. This call is part of a long-term strategic vision to build a safer and fairer internet. (Microsoft, 2025)

Conclusion

Ultimately, this study revealed that proactive leadership is essential for making AI effective in cyber crises. As digital attacks become increasingly sophisticated, merely responding and reacting is no longer sufficient to protect an organization. Instead, it is necessary to develop a model based on prediction rather than traditional reactive leadership. Proactive leaders are adept at leveraging technology and making strategic changes that integrate tools into the organizational culture. They prioritize early investment decisions and design early warning systems.

Real-world examples discussed in this study, such as Microsoft's response to the SolarWinds attack and Darktrace's use of adaptive artificial intelligence, demonstrate how proactive leaders utilize technology to create robust defense systems. Thus, it is not only the efficiency of the technology itself but primarily the leadership vision that guides its use and transforms artificial intelligence into a powerful defense mechanism.

5. Recommendations

To enhance organizational resilience against cyber threats, the following recommendations are proposed:

- Enhance Leadership Awareness of Technology: Leaders should stay informed about the latest technological advancements and their implications for cybersecurity.
- Adopt a Zero Trust Model: Implement security policies based on the principle of "never trust, always verify," managed through proactive leadership.
- Integrate Artificial Intelligence into Contingency Plans: Incorporate AI tools into existing contingency frameworks to improve response capabilities.
- Build an Organizational Security Culture: Foster a culture of security awareness and responsibility throughout the organization.
- Promote National and International Cooperation: Encourage collaboration among organizations, governments, and international bodies to strengthen collective cybersecurity efforts.
- Invest in Early Detection Systems: Prioritize investments in technologies that enable early detection of potential threats.
- Develop a Legal and Ethical Framework for AI Use: Establish guidelines to ensure the ethical deployment of AI technologies in cybersecurity.

List of references:

- AO-22-104746. (2022, January 13). *Cybersecurity: Federal response to SolarWinds and Microsoft Exchange incidents*. U.S. Government Accountability Office. <https://www.gao.gov/products/gao-22-104746>
- Arnaud, L. (2022). *Cyber crisis management: How to respond to cyberattacks?* <https://www.erium.fr/en/how-to-deal-with-a-cyber-crisis/#cyber-crisis-definition>
- AURORA. (2025). *Proactive leadership defined*. <https://auroratrainingadvantage.com/leadership/key-term/proactive-leadership/>
- Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, 29(3), 430–439. <https://doi.org/10.1111/1468-5973.12347>
- Boin, A., & 't Hart, P. (2003). Public leadership in times of crisis. *Public Administration Review*, 63(5), 544–553. <https://doi.org/10.1111/1540-6210.00318>
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58. <https://doi.org/10.1145/1541880.1541882>
- Clayton, R. (2025, July 15). *Securing core cloud identity infrastructure: Addressing advanced threats through public-private collaboration*. CISA. <https://www.cisa.gov/news-events/news/securing-core-cloud-identity-infrastructure-addressing-advanced-threats-through-public-private>
- Crant, J. M. (2000). Proactive behavior in organizations. *Journal of Management*, 26(3), 435–462. <https://doi.org/10.1177/014920630002600304>
- Darktrace. (2017, May 15). *NHS agency successfully fought back WannaCry ransomware with Darktrace*. <https://www.darktrace.com/news/nhs-agency-successfully-fought-back-wannacry-ransomware-with-darktrace>
- Darktrace. (2025). *Achieve proactive cyber resilience across your stack*. <https://www.darktrace.com/platform>
- ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. <https://doi.org/10.2824/782573>
- Hax, A. C., & Majluf, N. S. (1991). *The strategy concept and process: A pragmatic approach* (2nd ed.). Prentice Hall. <https://bayanbox.ir/view/8293998338328366226/S1.pdf>
- IBM. (2025). *IBM QRadar*. <https://www.ibm.com/products/qradar>
- ISC2. (2024, October 31). *2024 ISC2 cybersecurity workforce study*. <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>

Jones, D. (2025, June 2). Microsoft, CrowdStrike, other cyber firms collaborate on threat actor taxonomy. *Cybersecurity Dive*.

<https://www.cybersecuritydive.com/news/microsoft-crowdstrike-other-cyber-firms-collaborate-on-threat-actor-taxon/749614/>

Microsoft. (2025). الحوسبة السحابية من أجل الخير العالمي: خارطة طريق لحوسبة سحابية موثوقة، مسؤولية وشاملة. https://news.microsoft.com/cloudforgood/_media/downloads/a-cloud-for-global-good-arabic.pdf

Paul Schoemaker. (1995). Scenario planning: A tool for strategic thinking. *Sloan Management Review*, 36, 25–40.

https://www.researchgate.net/publication/220042263_Scenario_Planning_A_Tool_for_Strategic_Thinking

Recorded Future. (2025). *Know what matters. Act first*.

<https://www.recordedfuture.com/>

Shain, W. (2020, December 16). SolarWinds post-compromise hunting with Azure Sentinel. *Microsoft Tech Community*.

<https://techcommunity.microsoft.com/blog/microsoftsentinelblog/solarwinds-post-compromise-hunting-with-azure-sentinel/1995095>

Stryker, C. (2024). *What is advanced analytics?* IBM.

<https://www.ibm.com/think/topics/advanced-analytics>

Threat Hunter Team. (2024, January 24). *The 2024 ransomware threat landscape*.

<https://www.security.com/threat-intelligence/ransomware-threat-landscape-2024>

Wu, C.-H., & Wang, Y. L. (2011). Understanding proactive leadership. In W. H. Mobley, M. Li, & Y. Wang (Eds.), *Advances in global leadership* (Vol. 6, pp. 299–314). Emerald. [https://doi.org/10.1108/S1535-1203\(2011\)0000006015](https://doi.org/10.1108/S1535-1203(2011)0000006015)