International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Affordable Incident Response Using Cloud-Based Open-Source Data Pipelines with Integrated Threat Intelligence Platforms

Vijay Kartik Sikha

Submitted: 07/09/2019 **Revised:** 20/10/2019 **Accepted:** 30/10/2019

Abstract: The incident response landscape has undergone significant transformations in recent years, driven by the escalating complexity and sophistication of cyber threats. This paper explores the evolution of incident response from static relational databases to dynamic, cloud-based solutions and NoSQL databases, and examines the role of threat intelligence platforms, machine learning, and automation in enhancing the speed and accuracy of incident response efforts. The paper also discusses the benefits and limitations of cloud-based and open-source solutions and highlights the importance of integrating various technologies and systems to create a comprehensive incident response strategy. The future of incident response is characterized by increased automation, integration, and innovation, and organizations must prioritize incident response and invest in the technologies and strategies that will enable them to detect, respond to, and mitigate cyber threats effectively.

Keywords: *Incident Response, Cybersecurity, Cloud-based Solutions, NoSQL Databases, Threat Intelligence Platforms, Machine Learning, Automation, Open-source Solutions, SIEM, Security Orchestration, Artificial Intelligence, Serverless Architectures, Cyber Threats, Data Analytics, and Response (SOAR)*

1. Introduction

Incident response is a crucial aspect of cybersecurity, focusing on identifying, analyzing, and mitigating threats to protect information systems and networks from damage or unauthorized access. It involves a series of coordinated steps designed to detect security breaches, contain incidents, recover from attacks, and prevent future occurrences. Effective incident response processes can significantly reduce the impact of security incidents, ensuring business continuity and safeguarding critical assets (Casey, 2011).

The incident response market has grown significantly in recent years, driven by the increasing number of sophisticated cyber threats. Organizations are now investing heavily in response strategies and solutions, particularly as cybercrime becomes more targeted and destructive (Liska & Gallo, 2016). In response to this demand, the market for incident response solutions has expanded rapidly, providing significant opportunities for solution providers. The shift towards cloud-based services and open-source platforms has also revolutionized the way incident response is managed, moving away from static relational databases to more dynamic, scalable NoSQL databases that can better handle the increasing volume and complexity of cyber threat data (Naseer, 2018).

Cloud-based solutions offer unique advantages for incident response, such as real-time monitoring, rapid scalability, and integration with threat intelligence platforms. This has allowed organizations to adopt more cost-effective incident response frameworks, leveraging open-source data pipelines and automated processes to enhance their cybersecurity defenses (Schmidt et al., 2012). By integrating threat intelligence platforms, organizations can correlate incident data with known threat indicators, improving the speed and accuracy of their response efforts. This evolution in incident response technologies has been critical in keeping pace with the ever-evolving landscape of cyber threats.

2. Evolution of Incident Response: From Static to Cloud-Based Solutions

The evolution of incident response has been significantly impacted by the transition from static systems, like relational databases (RDBMS), to dynamic, cloud-based solutions and NoSQL databases. Traditionally, RDBMS struggled with the

(vksikha@gmail.com), ORCID: 0009-0002-2261-5551

increasing volume and complexity of cybersecurity data, leading to slow response times and inefficiencies in handling unstructured data such as logs and network traffic (Bejtlich, 2013). The manual effort required for querying and analyzing large data sets resulted in delayed detection and response to cyber threats (Schmidt et al., 2012). The shift to NoSQL databases and cloud-based services has revolutionized incident response by providing greater flexibility, scalability, and real-time data processing capabilities. NoSQL databases handle vast amounts of unstructured data more efficiently, while cloud services offer scalable resources and integration with threat intelligence platforms, automating data collection and analysis (Dionísio, 2018). This transition has not only enhanced the speed and accuracy of threat detection but also made advanced incident response tools more accessible to organizations of all sizes, improving overall security postures and minimizing breach impacts (Casey, 2011).

3. Ransomware Trends and the Need for Advanced Incident Response

In recent years, ransomware has emerged as one of the most damaging forms of cybercrime, with attacks increasing in both frequency and severity. Ransomware, a type of malware that encrypts a victim's data and demands a ransom for decryption, has proliferated due to factors such as heightened reliance on digital infrastructures, the rise of remote work, and advanced cybercriminal tactics (Liska & Gallo, 2016). The frequency of these attacks surged dramatically, with incidents doubling in 2021 and continuing to escalate. The financial impact is severe, with ransoms often reaching millions of dollars, in addition to costs associated with downtime, loss of productivity, reputational damage, and regulatory fines (Naseer, 2018). Critical sectors such as infrastructure, healthcare, and government have been particularly targeted, highlighting the wide range of ransomware's impact.

Attackers have refined their methods, including the use of Ransomware-as-a-Service (RaaS) and double extortion tactics, where they demand ransom not only for decryption but also threaten to leak sensitive data (Liska & Gallo, 2016). These evolving tactics underscore the inadequacy of basic incident response plans, necessitating advanced solutions. Traditional response processes often struggle against the rapid spread of ransomware, making advanced incident response frameworks essential. These frameworks, integrated with threat intelligence platforms, utilize real-time monitoring, automation, and analytics to detect and neutralize threats swiftly (Bejtlich, 2013). Furthermore, proactive threat hunting and robust backup and recovery plans are crucial for effective response. The integration of cloud-based open-source solutions and threat intelligence feeds helps organizations stay ahead of ransomware trends and enhance their security posture, highlighting the necessity for sophisticated incident response strategies as ransomware continues to evolve (Dionísio, 2018).

4. Key Components of Modern Incident Response Solutions

Modern incident response solutions are composed of several critical components that work together to detect, analyze, and mitigate security threats effectively. Key components include syslog aggregators, log parsers, threat intelligence databases, and automated response mechanisms. Each element plays a significant role in ensuring a comprehensive incident response strategy is in place to address cybersecurity incidents.

4.1 Syslog Aggregators

Syslog aggregators serve as the backbone for collecting log data from various sources within an organization’s IT environment. These tools gather, store, and manage log files from various devices, such as servers, firewalls, and routers, facilitating real-time monitoring of security events. By centralizing log data, syslog aggregators enhance visibility into potential security threats, enabling analysts to perform more thorough investigations (Suh-Lee, 2016).

4.2 Log Parsers

Log parsers analyze raw log data and convert it into a structured format that can be more easily processed and understood. This component is crucial for interpreting log entries from diverse systems and identifying patterns or anomalies that may indicate security breaches (Suh-Lee, 2016). Effective log parsing increases the efficiency of incident response by allowing security teams to focus on the most relevant log entries that require further examination.

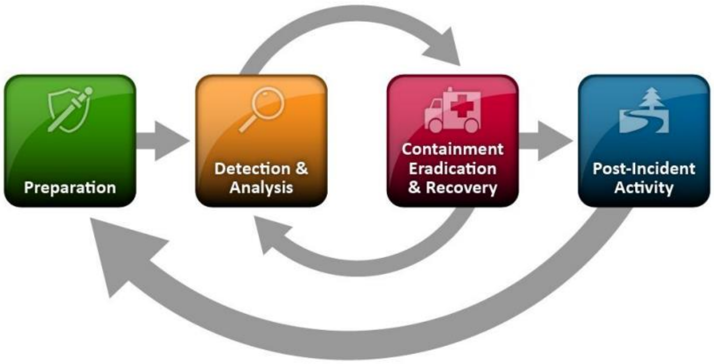
4.3 Threat Intelligence Databases

Threat intelligence databases compile and store information regarding known threats, vulnerabilities, and indicators of compromise (IOCs). This component supports incident response by providing real-time context to logged events, allowing security analysts to correlate data against recognized threat patterns. The integration of threat intelligence enhances the organization's ability to predict and proactively defend against emerging threats (Fetjah et al, 2016).

4.4 Automated Response Mechanisms

Automated response mechanisms are designed to execute predefined actions automatically in response to detected threats (Fetjah et al, 2016). This feature streamlines incident response processes by reducing the time it takes to react to security incidents, which can significantly mitigate potential damage. Automation also minimizes human error and ensures that appropriate responses are consistently executed.

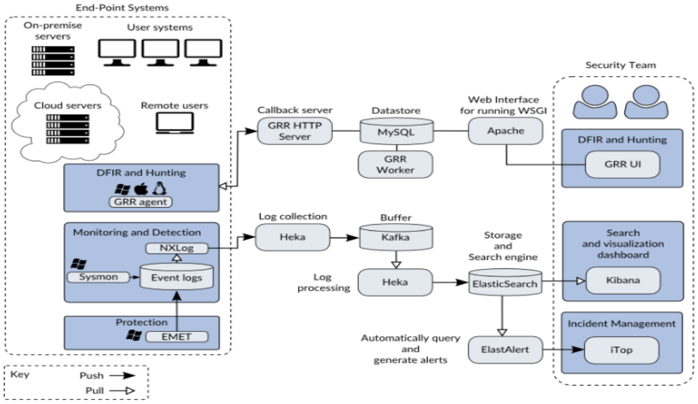
4.5 Incident Response Lifecycle:



Source: (Cichonski et al., 2012)

The image illustrates the four phases of the incident response lifecycle: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The preparation phase equips the organization with the necessary tools, policies, and training to handle security incidents. In the detection and analysis phase, potential incidents are identified and assessed. The containment, eradication, and recovery phase involves limiting damage, removing the threat, and restoring normal operations. Finally, post-incident activity includes reviewing the incident and implementing improvements. This process is continuous, with each phase informing the next to enhance future responses.

4.6 Example: Architecture Diagram for Incident Response



Source: (Summit Route - Iterative Defense Architecture, 2015)

The architecture diagram illustrates a comprehensive Endpoint Detection and Response (EDR) system, integrating various components to ensure robust security and efficient incident management. It begins with on-premise and remote user systems connecting to cloud servers, which handle Digital Forensics and Incident Response (DFIR) and hunting processes. Logs are collected and processed using Heka, buffered with Kafka, and stored in Elasticsearch, with visualization through Kibana. The security team interacts with the system via a web interface running on Apache, connected to the DFIR and hunting components. Additionally, the system includes incident management tools like ElastAlert and iTop for generating alerts and managing incidents effectively. This setup ensures a seamless flow of data and efficient handling of security incidents.

5. Leveraging Modern Technologies for Ad-Hoc Incident Response Solutions

With the increasing complexity of cyber threats, organizations require flexible and scalable incident response solutions that can be deployed rapidly during unexpected security events. Modern cloud-based technologies and open-source data pipelines are playing a critical role in creating ad-hoc incident response systems that are not only cost-effective but also highly adaptive to changing threat environments. These solutions are designed to handle large volumes of data in real-time, integrate with threat intelligence platforms, and automate responses, thereby improving an organization’s ability to mitigate security incidents promptly.

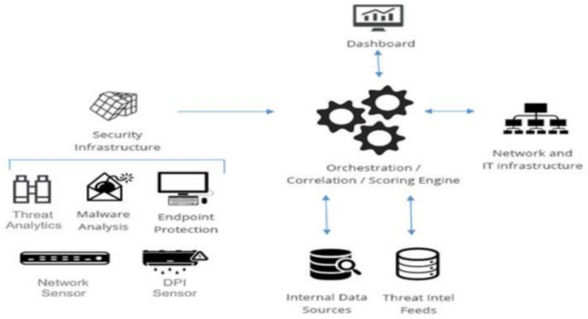
Cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud have become the backbone for many incident response frameworks. They offer the flexibility to deploy and scale security solutions on-demand, minimizing the need for significant upfront infrastructure investment.

5.1 Case study Netflix's Incident Response Using Cloud and Open Source Solutions

A notable example of leveraging modern technologies for incident response before 2018 is **Netflix**, a pioneer in cloud technology and a heavy user of **AWS**. In 2017, Netflix faced increasing cybersecurity threats targeting their streaming services. They needed a real-time monitoring and incident response solution that could handle massive amounts of data generated by their global user base (Netflix Technology Blog, 2017).

Netflix developed **The Security Monkey**, an open-source tool integrated with AWS, that monitored their cloud environment for security misconfigurations and unauthorized access. The system used **Elasticsearch** and **Kibana** to visualize log data and facilitate quick detection of suspicious activity. By implementing an open-source solution integrated with AWS services, Netflix was able to detect and remediate security issues within minutes rather than hours (Netflix Technology Blog, 2017).

The architecture allowed Netflix to scale their security monitoring as their infrastructure grew and adapted to changing threat landscapes. This approach not only provided rapid incident detection and response but also reduced the need for large capital expenditures typically associated with on-premises solutions. As a result, Netflix was able to maintain the security of its cloud environment while continuing to expand its services (Netflix Technology Blog, 2017).



Netflix open sources FIDO (Source: Zeljka Zorz, 2015)

6. Cost and Time Comparison: Past vs. Present Incident Response

Incident response (IR) processes have evolved significantly, driven by technological advancements and changes in organizational infrastructure. Historically, IR was a costly and resource-intensive endeavor, reliant on static relational databases and manual processes, which led to slow response times and high expenses (Romanosky, 2016). Organizations invested heavily in on-premise hardware and proprietary software licenses, with dedicated security information and event management (SIEM) systems requiring significant capital and maintenance costs. Manual log analysis and response efforts often resulted in detection and response times spanning days or even weeks, increasing the potential for damage and associated costs (Gartner, 2016).

In contrast, modern IR has become more efficient and cost-effective due to the adoption of cloud-based and open-source technologies. Cloud platforms like AWS, Microsoft Azure, and Google Cloud offer scalable infrastructure that can be rapidly deployed in response to incidents, while open-source tools such as Apache Kafka, Elasticsearch, and Suricata enable real-time monitoring and automated responses (Fetjah et al., 2016). These advancements eliminate the need for expensive hardware and proprietary software, reducing both costs and response times. Automation has further accelerated incident detection and containment, with modern solutions achieving response times within minutes or hours, compared to the days required in the past. Studies indicate that automated and cloud-based IR solutions can reduce response times by up to 90% and lower recovery costs significantly (Thompson, 2018).

6.1 Cost Comparison of Tools

The cost savings between past and present incident response (IR) solutions are substantial. Historically, organizations faced significant expenses for hardware, proprietary software licenses, and dedicated security teams. For instance, a traditional SIEM system could cost hundreds of thousands of dollars annually, excluding maintenance, upgrades, and staffing costs (Cichonski et al., 2012). In contrast, modern cloud-based services and open-source tools offer a more cost-effective approach. Platforms like AWS and Google Cloud operate on a pay-as-you-go model, eliminating the need for substantial upfront investments. Open-source tools such as Elasticsearch and Logstash provide robust data indexing and log management capabilities without the high licensing fees of proprietary software, enabling organizations to implement comprehensive IR solutions at a fraction of the cost of legacy systems (Schmidt et al., 2016).

6.2 Time Comparison: Legacy vs. Cloud-Based Incident Response

Legacy incident response (IR) systems required security teams to spend extensive time manually collecting and correlating data. With the introduction of automated cloud-based solutions, the time needed for incident detection, analysis, and response has been significantly reduced. For example, Netflix’s Security Monkey tool automates the monitoring and correction of security misconfigurations in real-time, a process that previously took hours or days manually (Naseer, 2018). Modern tools integrated with threat intelligence platforms can automatically identify known threats and initiate remediation actions without human intervention. This advancement not only accelerates response times but also allows security teams to focus on strategic tasks like threat hunting and enhancing security postures (Suh-Lee, 2016).

7. Essential Integrations for Successful Incident Response Solutions

A successful incident response (IR) solution relies on integrating various technologies and systems to enable comprehensive monitoring, detection, and mitigation of cybersecurity threats. Key integrations include Security Information and Event Management (SIEM) solutions, Active Directory (AD), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), threat intelligence platforms, Endpoint Detection and Response (EDR), and Security Orchestration, Automation, and Response (SOAR) systems.

SIEM systems are central to IR solutions, aggregating and correlating data from multiple sources to provide a unified view of security events and enable real-time analysis (Schmidt et al., 2016). Common SIEM solutions like Splunk, IBM QRadar, and ArcSight integrate with other tools to offer automated alerting and response capabilities (Gartner, 2016). Active Directory integration is crucial for managing user identities and detecting unauthorized access, with automated responses triggered by suspicious activities (Liska & Gallo, 2016).

IDS and IPS systems monitor and protect network traffic from malicious activities, such as malware and denial-of-service attacks (Naseer, 2018). Tools like Snort and Suricata, used with SIEM platforms, help detect and respond to threats in real-time (Bejtlich, 2013). Integrating threat intelligence platforms into IR solutions enhances threat detection by correlating real-time events with known attack vectors (Dionísio, 2018). Platforms such as Recorded Future and ThreatConnect offer valuable insights into emerging threats.

Endpoint Detection and Response (EDR) tools, like CrowdStrike Falcon and Carbon Black, monitor and analyze endpoint activities to detect and respond to threats (Thompson, 2018). Integrating EDR with SIEM and threat intelligence platforms allows for automated responses to endpoint threats. SOAR platforms, including Palo Alto Networks Cortex XSOAR and Splunk Phantom, further streamline incident response by automating repetitive tasks and improving the efficiency of security operations centers (Cichonski et al., 2012).

8. Incident Response Capabilities in Enterprise Solutions

Incident response (IR) capabilities in enterprise solutions are highly sophisticated and offer comprehensive tools and automation features that enable large organizations to effectively detect, analyze, and respond to cybersecurity threats. These enterprise-grade solutions are designed to integrate seamlessly with existing security infrastructure and provide advanced analytics, orchestration, and automation features that enhance the overall incident response process.

8.1 Pros of Enterprise Solutions

Enterprise incident response (IR) solutions offer several advantages, notably in integration, threat detection, compliance, and support. These solutions provide comprehensive integration with various security tools, such as Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR), and Security Orchestration, Automation, and Response (SOAR) platforms. For example, IBM Resilient, Splunk Enterprise Security, and Palo Alto Networks Cortex XSOAR facilitate streamlined workflows and automated response actions, reducing the need for human intervention and minimizing response times (Gartner, 2016).

Advanced threat detection and analysis are enhanced through the incorporation of machine learning and artificial intelligence in enterprise IR solutions. Tools like FireEye Helix and Microsoft Sentinel leverage these technologies to automatically correlate data, detect sophisticated attack patterns, and provide actionable insights (Bejtlich, 2013). Additionally, enterprise solutions support regulatory compliance with preconfigured templates for standards such as GDPR, HIPAA, and PCI-DSS, simplifying reporting and audit processes (Cichonski et al., 2012).

8.2 Cons of Enterprise Solutions

Enterprise incident response (IR) solutions come with notable drawbacks, primarily in terms of cost, complexity, and vendor lock-in. One significant disadvantage is their high cost, including licensing fees, subscription charges, and ongoing support and maintenance, which can be prohibitively expensive for small to mid-sized organizations. Solutions like Splunk and IBM Resilient are particularly costly, making them more suitable for large enterprises with substantial cybersecurity budgets (Schmidt et al., 2016).

Additionally, these solutions can be complex to implement and maintain, often requiring specialized personnel for effective management. The complexity of enterprise IR systems can lead to extended implementation periods and a higher risk of configuration errors (Thompson, 2018). Furthermore, enterprise solutions may lead to vendor lock-in, as they often require deep integration with tools from the same vendor, restricting flexibility and complicating the integration of third-party solutions as organizational needs change.

8.3 Incident Response Capabilities in Open-Source Solutions

Open-source incident response (IR) solutions offer a cost-effective and flexible alternative to enterprise-grade tools, although they come with their own set of advantages and limitations. One of the most significant benefits is cost-effectiveness, as open-source tools like TheHive and MISP are free to use, eliminating the need for expensive licensing fees (Dionísio, 2018). These solutions also offer high customizability, allowing organizations to modify and extend the software to fit their specific needs, thanks to the open availability of source code (Fetjah et al., 2016). Additionally, open-source IR tools benefit from active community support, where developers and users collaborate to enhance functionality and troubleshoot issues, promoting continuous improvement (Naseer, 2018). Furthermore, many open-source tools are lightweight and scalable, suitable for various organizational sizes and deployment environments.

However, open-source solutions often have limitations compared to their enterprise counterparts. They may lack advanced features and integrations, such as sophisticated machine learning capabilities or automated playbooks, and typically do not come with official customer support, which can be crucial during critical incidents (Suh-Lee, 2016). Additionally, these tools often require manual setup, configuration, and maintenance, which can be time-consuming and dependent on community-driven updates (Bejtlich, 2013). Furthermore, open-source software present potential security vulnerabilities, as publicly accessible code may be exploited by malicious entities if not adequately managed, necessitating vigilant patch management and robust security protocols (Cichonski et al., 2012).

9. Market Leaders & Innovation in Incident Response

The incident response (IR) market has witnessed significant advancements and innovations from leading companies, reflecting the growing complexity of cyber threats and the need for more sophisticated response solutions. As of January 2019, several companies have emerged as market leaders, driving innovation through advanced technologies and integrated solutions. This section explores the contributions of these key players and highlights their role in shaping the future of incident response.

9.1 Leading Companies and Innovations

IBM Security

IBM Security is a prominent leader in the IR space, offering a comprehensive suite of solutions designed to enhance threat detection and response capabilities. IBM's QRadar Security Information and Event Management (SIEM) platform is widely recognized for its ability to provide advanced analytics and real-time visibility into security events (Cahill, 2018). IBM has also made significant strides with its Resilient Incident Response Platform, which integrates automation and orchestration to streamline response workflows and improve operational efficiency (Cahill, 2018).

FireEye

FireEye is another key player known for its innovative approach to incident response. FireEye’s Helix Security Operations Platform combines threat detection, investigation, and response capabilities into a unified solution. The platform is designed to help organizations automate and accelerate their incident response processes by providing comprehensive visibility and actionable insights (Kavanagh et al., 2015).

Splunk

Splunk is widely recognized for its data analytics and visualization capabilities, with its Splunk Enterprise Security solution offering powerful tools for incident detection and response. Splunk’s platform provides advanced analytics, machine learning, and visualization tools to help security teams gain deeper insights into security events and incidents (Robb, 2018).

10. Machine Learning in Advanced Threat Analysis and Forensics

Machine learning (ML) has revolutionized threat analysis and forensics within incident response frameworks, offering advanced capabilities in anomaly detection, predictive analytics, and automated threat classification. ML excels at anomaly detection by identifying deviations from normal behavior that traditional rule-based systems might miss. For instance, Elastic Security and Darktrace use ML to detect unusual network activities and insider threats, respectively, by analyzing deviations from established baselines and normal behaviors (Thompson, 2018). Predictive analytics, powered by ML, forecasts potential threats by analyzing historical data, helping organizations implement preventive measures. Cisco’s Cognitive Intelligence and IBM QRadar Advisor with Watson demonstrate this by predicting emerging threats and offering mitigation strategies based on historical and current data (Bejtlich, 2013; Schmidt et al., 2016). Additionally, ML automates threat classification, streamlining the categorization and prioritization of security incidents. CrowdStrike Falcon and FireEye’s Helix utilize ML for this purpose, improving response times and accuracy (Cichonski et al., 2012). Future developments may include more sophisticated models and integration with emerging technologies, further enhancing ML’s role in cybersecurity (Naseer, 2018).

Case Study: Darktrace

Darktrace leverages its proprietary AI technology, the Enterprise Immune System, to detect and respond to cyber threats in real-time (Darktrace, 2019). This system mimics the human immune system by identifying anomalies based on learned behaviors of users and devices within a network. It continuously monitors network traffic and user activity to establish a baseline of "normal" behavior. When deviations occur—such as unusual login times or unauthorized access attempts—the system flags these anomalies as potential threats. Darktrace's self-learning capabilities enable the technology to adapt over time, improving its ability to differentiate between benign anomalies and genuine threats, thus reducing false positives. In cases of confirmed threats, Darktrace can automatically respond by isolating affected accounts or devices to mitigate damage. Organizations using Darktrace have reported faster incident response times, enhanced threat intelligence, and improved operational efficiency (Darktrace, 2019). This case highlights how machine learning and AI can significantly enhance incident response capabilities, making them essential tools for organizations facing increasingly sophisticated cyber threats.

11. Conclusion

In conclusion, the incident response landscape has undergone significant transformations in recent years, driven by the escalating complexity and sophistication of cyber threats. The evolution from static relational databases to dynamic, cloud-based solutions and NoSQL databases has revolutionized incident response, enabling organizations to detect and respond to threats more effectively. The integration of threat intelligence platforms, machine learning, and automation has further enhanced the speed and accuracy of incident response efforts.

The increasing adoption of cloud-based and open-source solutions has democratized access to advanced incident response capabilities, making them more accessible to organizations of all sizes. The Netflix case study exemplifies the benefits of leveraging modern technologies for incident response, demonstrating the potential for rapid detection and remediation of security issues.

As the threat landscape continues to evolve, it is essential for organizations to adopt a proactive and adaptive approach to incident response. This involves integrating various technologies and systems, such as SIEM, threat intelligence platforms, and automation tools, to create a comprehensive incident response strategy.

The future of incident response will be shaped by emerging technologies, including machine learning, artificial intelligence, and serverless architectures. Open-source collaborations will continue to drive innovation, and the development of more sophisticated models and integrations with emerging technologies will further enhance the role of machine learning in cybersecurity.

However, as the incident response market continues to grow and mature, it is crucial to acknowledge the limitations and challenges associated with certain solutions. The trade-offs between cost, complexity, and vendor lock-in must be carefully considered, and organizations must be prepared to adapt their incident response strategies to address the evolving threat landscape.

Ultimately, the future of incident response will be characterized by increased automation, integration, and innovation. As organizations continue to face an ever-changing threat landscape, it is essential to prioritize incident response and invest in the technologies and strategies that will enable them to detect, respond to, and mitigate cyber threats effectively.

References

[1] Bejtlich, R. (2013). The practice of network security monitoring: understanding incident detection and response. No Starch Press.

[2] Cahill, P. (2018, October 18). *IBM QRadar: The Intelligent SIEM - IBM Nordic Blog*. IBM Nordic Blog. https://www.ibm.com/blogs/nordic-msp/ibm-qradar-the-intelligent-siem/

[3] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

[4] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

[5] Dionísio, N. R. M. (2018). Improving cyberthreat discovery in open source intelligence using deep learning techniques (Doctoral dissertation).

[6] Fetjah, L., Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said Jai-Andaloussi, & Abderrahim Sekkaki. (2016). *Toward a Big Data Architecture for Security Events Analytic*. https://doi.org/10.1109/cscloud.2016.53

[7] Gartner. (2016, April 7). *How to Plan and Execute Modern Security Incident Response*. Retrieved from https://www.gartner.com/en/documents/3277828

[8] Kavanagh, K. M., Rochford, O., & Bussa, T. (2015). Magic quadrant for security information and event management. Gartner Group Research Note.

[9] Liska, A., & Gallo, T. (2016). Ransomware: Defending against digital extortion. " O'Reilly Media, Inc.".

[10] Naseer, H. (2018). A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility (Doctoral dissertation, PhD Dissertation (Melbourne: School of Computing and Information System, The University of Melbourne).

[11] Netflix Technology Blog. (2017, August 21). *A Brief History of Open Source from the Netflix Cloud Security Team*. Medium; Netflix TechBlog. https://netflixtechblog.com/a-brief-history-of-open-source-from-the-netflix-cloud-security-team-412b5d4f1e0c

[12] Robb, D. (2018, October 5). *Splunk Enterprise Security Review: SIEM Features & Pricing*. ESecurity Planet. https://www.esecurityplanet.com/products/splunk-enterprise-security-es/

[13] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001–tyw001. https://doi.org/10.1093/cybsec/tyw001

[14] Schmidt, K., Phillips, C., & Chuvakin, A. (2012). Logging and log management: the authoritative guide to understanding the concepts surrounding logging and log management. Newnes.

[15] Suh-Lee, C. (2016). *Mining Unstructured Log Messages for Security Threat Detection*. Digital Scholarship@UNLV. https://digitalscholarship.unlv.edu/thesesdissertations/2749/

[16] *Summit Route - Iterative Defense Architecture*. (2015). Summitroute.com. https://summitroute.com/blog/2015/06/13/iterative_defense_architecture/

[17] Thompson, E. C. (2018). The Significance of Incident Response. *Apress EBooks*, 1–10. https://doi.org/10.1007/978-1-4842-3870-7_1

[18] Zeljka Zorz. (2015, May 6). *Netflix open sources FIDO, its automated incident response tool - Help Net Security*. Help Net Security. https://www.helpnetsecurity.com/2015/05/06/netflix-open-sources-fido-its-automated-incident-response-tool/

[19] Darktrace. (2019, September 9). *Darktrace launches Enterprise Immune System Version 4*. Darktrace. https://darktrace.com/news/darktrace-launches-enterprise-immune-system-version-4