ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Real-Time Incident Response and Remediation-A Review Paper

Ankur Mahida

Subject Matter Expert (SME), Barclays, USA

ABSTRACT

The real-time correlation of IRR to effective cyber defense plays a crucial role. Regular answers usually take more time to be provided and permit devastations to occur, thus becoming more severe. The swiftest IRR of automation and real-time analytics is characterized by early threat detection, instant response, and quick incident resolution. The very needed capabilities include machine detection of abnormalities and threats, quick investigation through correlation and AI, and fast response through preinstalled playbooks. SIEM, EDR, and SOAR operationalization make active IRR possible in real-time. The positive aspects of introducing such a solution are pronounced - early threat containment, speedy recovery, and higher efficiency levels for the security team. On the other hand, actual-time IRR has limitations: false positives, integration of faiths, people and procedures dependence, and effectiveness against advanced threats. However, inundation by the real-time IRR signifies a cybersecurity revolution. The real-time IRR is an opportunity for innovation in analytics and automation that partially or transforms the enterprise security system. However, the dissemination faces technical and coordination-related barriers. The real-time IRR capability is a clear sign of progress in eliminating the cyber resiliency gap, but there is still room for improvement to achieve the best.

***Corresponding author**

Ankur Mahida, Subject Matter Expert (SME), Barclays, USA.

Received: April 13, 2023; **Accepted:** April 18, 2023; **Published:** April 24, 2023

Keywords: Real-Time, Incident Response, Remediation, Cybersecurity

Introduction

The term real-time incident response and remediation (IRR) describes the ability to automatically detect cyber threats in real time and then react rapidly to stop the attacks and recover any damage fast. Up-to-the-minute IRR is a must for modern cyber defenses since the old-school response is too sluggish to deal with speedily-spreading attacks. Real-time monitoring and quick response are the keys to the success of well-functioning security operations. The issue of how to do IRR in real-time became critical after the coming of fast-propagating worms and zero-day exploits. Over these years, major technological breakthroughs in security analytics, endpoint monitoring, and automation have finally catalyzed the real-time implementation of IRR. Like Security Information and Event Management (SIEM) solutions, real-time data analytics is used for threat correlation [1]. Endpoint detection and responses (EDR) continuously monitor endpoints. Security Orchestration, Automation, and Response (SOAR) platforms enable real-time playbook execution at the time of instant responses [2]. There is a combined effect of these technologies on the key IRR capabilities in real-time, which are automatic threat alerting, brisk investigation, and immediate containment and remediation. IRR in real-time is a big step toward cyber-attack defenses, but still, many capabilities are being developed.

Problem Statement

The old incident response relies on manual procedures that need to be faster and, per technology, defeated to meet the needs of the current cybercrime threats. Typically, most organizations still apply a stepwise incident response plan, which progresses through separate stages like discovery, investigation, containment, extinction, and recovery [3]. The structure of this note may take several hours to finish. Nevertheless, modern threats, which are fast propagating, imply a vast potential to compromise the entire network in minutes and spread more quickly than DNS tunneling attacks. Such characteristics as "zero days" and advanced persistent threats employ the fact of the unknown vulnerabilities and evade the primary security control instruments. The longer response time from the single manual handling is why attackers can penetrate deep across the network and bring havoc.

The gap between existing manual response and the speed and capabilities of the current sophisticated threats has made it clear that traditional incident response needs to catch up. Often, there are delays in the discovery of failings and breaches. Whenever an alert arises, the security department manually handles it, gathering system evidence like logs, analyzing the data, and determining the breach extent. In addition, manual containment and remediation also take place, putting human lives at risk in case they infect others. This low reaction speed of human-driven incident response is a significant cause of undesirable downtime and recovery costs in the present scenario.

Real-time action for incidents and remediation can be laborious because of the heavy bias purpose for manual work and the absence of adequate technologies [4]. Organizations agree they must be able to detect incidents in real time, respond automatically, and make instant decisions, but capabilities gaps surround identification, investigation, and rapid response. Modernizing traditional incident response processes while simultaneously adopting future-oriented technologies such as security analytics, endpoint monitoring, and automation necessitates funding. An advanced cybersecurity

system requires critical consideration of the weaknesses inherent in the traditional response models to provide a sophisticated response to modern threats.

Solution

In RRIR (Real-time incident response and remediation), intelligent automation provides a broad spectrum of functionalities that address one of the critical weaknesses in the traditional response strategy [5]. The center of attention is to change from cumbersome and manual processes to quick-witted multipurpose people and successful capacities that can immediately detect, investigate, and counteract incidents. Instantaneous IRR desires to check threats in minutes, whereas traditional IRR seeks interventions after a few days or weeks.

The primary true-time feature imperative is machine intelligence, auto-correlation, and automatic instant response technology. The capabilities of security analytics solutions like SIEM revolve around correlating events and spotting unusual behavior in real time to identify dangers [6]. AI and machine learning algorithms can also detect well-known and malicious attack patterns. Endpoint detection and response (EDR) has continually been tracking the endpoints to catch behavioral threats; its event detection capability and effectiveness simplify remediation [6]. Automated playbooks provided by using the SOAR technology platform feature quick response by carrying out the current workflows (containment, mitigation) or only after people supervise.

Several technologies are fundamental for enabling real-time IRR: Several technologies are essential for allowing real-time IRR:

- The SIEM (Security Information and Event Management) provides real-time analytics power and processes to correlate to find IOCs and threats in the entire enterprise [7].
- EDR solution (Endpoint Detection and Response) works with activity monitoring of endpoints and leverages behavioral analysis to bring out attacks that bypass ordinary control barriers [7].
- Security Orchestration, Automation, and Response (SOAR) help construct playbooks that, when triggered, can enact processes aimed at containing threats instantly [8].
- AI and machine learning approaches are based on techniques that detect hidden threats and unusual actions to address stealthy attacks [9].

Combining the two technologies produces, in this case, the automated tools that can overturn the past mode of dealing with incidents, turning them into a real-time process. AI with real-time Irr is rapidly shrinking the time taken while reducing the need for the manual method for investigation and containment.

Impact

The real-time incident response makes it possible to determine threats quickly through continuously scanning the environment. Modern data system is susceptible to many cyber security threats which can comprise of a virus attack, data breaches and denial-of-service (DoS). Cyber criminals exploit different types of high-tech (e.g: phishing, social engineering etc) methods to hack into sensitive data without authorization and steal intellectual property [9]. The Security Information and Event Management (SIEM) solutions will provide services like the ingestion and the correlation of the data in real-time for the indicator of compromise (IOCs) and anomalies, these services are the notable importance to business using this service. Endpoint detection and response (EDR) tools make endpoint activity monitoring a part of their operations whenever they spot unusual behaviors and attacks [10]. Machine learning with artificial intelligence techniques allows the search of new threats not corresponding to signatures of the old ones. At the same time, the trialing of cybersecurity devices provides the opportunity to view within minutes or seconds of virus attacks rather than days after the damage.

Detecting threats and containing the outbreaks affecting both on-premise and cloud infrastructures by automatically isolating issues with appropriate response playbooks are the two actions of this remedy [11]. This could be blocking user accounts, ceasing services, or disabling IPs, URLs, or hallway endpoints. In this regard, a practical approach is to contain the explosion within minutes and prevent the expansion of an explosion zone. SOAR platforms provide automated response playbooks to minimize disruption and downtime for quick recovery.

This entails the functionality that an alert system can go back to situations where unauthorized changes have occurred, including the rolling-out of encryption of an encrypted device or the ransomware's configuration. Such malware removal, system restore, and password reset methods can be automated for immediate recovery and restoration. Due to the achievement of compliance through prompt execution of the requirements, the benefits include response and mitigation.

Front-rank over-watching allows machine learning algorithms to recognize deviations in enterprise behavior patterns and security issues. This guarantees enhanced monitoring by security teams, who can detect signs of compromise. Sharing intelligence with all the partners and exchanging threats prevents hackers from hiding from within the black web; however, with global IOCs, hackers would be exposed. The security team can heighten threat detection, response, and recovery ease through enhanced modernization.

Cyber incident response systems can accurately predict cyber threats in real-time, thus allowing for early detection and containment, dramatically reducing the damage caused by cyberattacks [12]. Organizations have had a significant loss during the réprochement of crash breaches. Real-time capabilities in setting the crisis plan will cut down the scale of damage and equally expand towards aiding the company's disruption, recovery, and reputation. Rapid reaction time to down-spiral and recovery processes helps accelerate recovery after incidents. Automation remarkably improves performance by reducing the number of manual investigations and remediations that need to be done. The real-time response reports suggest that the security fast can be lowered by almost half while the response is accessed by 90%.

Through integrating detection processes, response mechanisms, and resilience, IRR provides a continuous boost to the security posture of a hybrid enterprise [13]. It provides the basis for higher cyber maturity. Read on for the full transcript. Cyber security awareness becomes paramount now that we are operating in the digital environment, as it allows the individual citizen to control his or her private life and responsibilities in cyberspace. Privacy plays a crucial role throughout this experience since character impersonates him/her/them. Living every moment in the digital space, we create a digital footprint that could help all organizations attain certain advantages over competitors if they don't go for real-time systems. The risks of breaches can be reduced, and faster recovery times can be achieved. Companies' massive adoption of real-time IRR to guard against any cyber threat can be a game changer in cyber defense capabilities and survivability.

To reap such advantages, set aside a budget to purchase equipment, streamline operations, develop business processes, and recruit talented workers. Achievement of the goals consists of many factors, such as increasing response times, reducing containment times, and lowering the dwell time and the recovery costs. The principle seems bright that live IRR brings to this process a revolution that ensures an efficient decision-making process and improves a sense of security in the long term.

Nevertheless, despite that, businesses should aim to modernize the processes, adopt transformative technologies, and achieve high levels of expertise on the ground to maximize these benefits. Reducing response times, relevant containment rate measurements, and recovery price index are the principal metrics of the actual IRR impact. However, the picture is foreseen to be very bright for revolutionary cyber defense as real-time possibilities start speeding up.

Scope and Limitation

While the capabilities of real-time IRR are expanding rapidly, there are still some constraints on the scope and limitations to consider:

- **Enterprise Focus:** RIT ensures that the IT of companies, networks, and endpoints remain free of threat. Incident response capabilities for false positives from the cloud, ICS\ OT, and other technologies are improving.
- **False Positives:** The over-sensitivity of real-time analytics may also trigger alert fatigue, ultimately leading to healthcare fraud control inefficiencies. From a cognitive point of view, scanning is filtering out irrelevant stimuli and attending to the actual threats.
- **Integration Issues:** Security tools work individually, not communicating with each other, requiring a solid integration for real-time ingestion, correlation, and response workflows.
- **Human Dependence:** Highly experienced analysts are still needed to interpret alerts and operate the systems while managing complex responses. Automation does not replace human thought, nor does it dismantle human oversight.
- The insider threats ensure the effectiveness of existing systems in identifying and overcoming the impact of privileged access users performing malicious activities.
- **Hybrid Threats:** Many attacks now look differently from the species that had previously prompted the implementation of phalanx-type defenses due to multi-potential malware. Analytics, automation, and processes require a repetitive upgrade to detect more elaborate threats.

Instantaneous attack identification, recognition, and remediation need to be improved and are still critically limited owing to many factors IRR attempts to cover, resulting in the scope of protection issues. Steadily and continuously advancing technology and a set of good practices are the main things that will help to enhance abilities and overcome the restrictions.

Conclusion

Overall, incident response and remedy in real-time have become the most critical breakthroughs in cybersecurity. With automation, analytics, and orchestration, threats are responded to quickly; they are contained and recovered, exceeding the standard, slow response. The real-time advanced mode of IRR will help prevent a breach and speed up the recovery, increasing the defense's authority. However, technological inventions and scientific research are needed to identify new applications and enhance capabilities to draw out their full potential. Organizations face several adoption barriers, including integration complexity, knowledge building, and the creation of new processes. But the future expectation is reasonable when real-time IRR solutions evolve and grow. For instance, the use of SIEM and EDR merging with SOAR allows organizations to progress on their maturity level of response competence. The cooperation of vendors and practitioners will solve the current shortcomings; time-based is about to be a game changer, venting advanced threats and taking care of enterprise resilience.

References

1. Granadillo GG, Zarzosa SG, Diaz R (2021) Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 21: 4759.
2. Islam C, Babar MA, Nepal S (2019) A Multi-Vocal Review of Security Orchestration. ACM Computing Surveys 52: 1-45.
3. Xi D DZ, Taylor SW, Woolford DG, Dean CB (2019) Statistical Models of Key Components of Wildfire Risk. Annual Review of Statistics and Its Application 6: 197-222.
4. Javed AR, Shahzad F, Rehman S, Zikria YB, Razzak I, et al. (2022) Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. Cities 129: 103794.
5. Wang M, Wang B, Abareshi A (2020) Blockchain Technology and Its Role in Enhancing Supply Chain Integration Capability and Reducing Carbon Emission: A Conceptual Framework. Sustainability 12: 10550.
6. Vielberth M, Bohm F, Fichtinger I, Pernul G (2020) Security Operations Center: A Systematic Study and Open Challenges. IEEE Access 8: 227756-227779.
7. Najafi P, Cheng F, Meinel (2021) CSIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management. Springer eBooks 25-43.
8. Wittkop J (2022) The Cybersecurity Playbook for Modern Enterprises : An End-To-end Guide to Preventing Data Breaches and Cyber Attacks. Birmingham: Packt Publishing, Limited https://www.packtpub.com/product/the-cybersecurity-playbook-for-modern-enterprises/9781803248639.
9. Granadillo GG, Dubus S, Motzek A, Alfaro JG, Alvarez E, et al. (2018) Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems 83: 535-552.
10. Karantzas G, Patsakis C (2021) An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy 1: 387-421.
11. Iansiti M, Lakhani KR (2020) Competing in the age of AI: strategy and leadership when algorithms and networks run the world. Harvard Business Review Press https://www.hbs.edu/faculty/Pages/item.aspx?num=56633.
12. Zhou C, Hu B, Shi Y, Tian Y C, Li X, et al. (2021) A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems. Proceedings of the IEEE 109: 517-541.
13. Rashid Z, Noor U, Altmann J (2021) Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. Future Generation Computer Systems 124: 436-466.