International Journal of Knowledge Based Computer Systems
13 (1) 2025, 31-37
www.publishingindia.com//ijkbcs/

Methodologies for Optimized Event and Incident Processing in Cybersecurity

Cheryl Ann Alexander[1*] and Lidong Wang[2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA.
Email: cannalexander68@gmail.com
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA.
Email: lidong@iser.msstate.edu
[*]Corresponding Author

Abstract: Cybersecurity is an essential function of all enterprises. Threat mitigation is necessary to prevent cyber risks from costing the enterprise much more money and resources. The enterprise should establish a robust and vigorous cybersecurity program. Every incident is an event but not every incident should demand an urgent response. Much of the value of incident processing and incident reporting lies in the free-text section of the incident report. In healthcare, incident processing is a key function of the IT department. By determining whether an attack's detection is imminent, IT can utilize threat mitigation to reduce costs and resources associated with cybersecurity threats. Artificial intelligence, big data, and machine learning have been utilized in threat mitigation. In healthcare, this is an essential function of the IT department to reduce the likelihood of Ransomware attacks. This paper discusses event processing, incident processing, and the tools used to mitigate any attacks.

Keywords: Artificial intelligence (AI), Cybersecurity, Healthcare, Incident processing, Information, System, Threat mitigation.

I. Introduction

Every incident constitutes an event and selected events should not demand an urgent response. Information concerning patient safety incidents has been broadly identified by incident reporting systems. The free-text section of incident reports constitutes much of the value of incident reports. To address the gravity of incidents within an enterprise, researchers developed a decision-making scoring system that determined the severity of incidents using the semantic features of the text in incident reports comparing the results with the opinions of experts. Next, researchers calculated a severity term score, a severity report score, and a severity group score. However, it is necessary to research and investigate a suitable number of incident reports necessary to evaluate groups utilizing the severity report score, therefore, further research is necessary. The data volume necessary to decide the trends corresponding to the tendencies of the central limit theorem is the key to this approach [1].

A collection of automated tools such as vulnerability scanners, monitoring and logging tools, and antivirus software has been investigated. Decision trees for each category of tools were executed to assist in finding the way through huge amounts of information [2]. Table I [3] shows some threats (with a high probability of incident occurrences) during the COVID-19 pandemic.

Table I: Some Threats During COVID-19

Aspects	Threats
Actions on objectives	Financial fraud, data theft, personal information theft, password stealer, ransom, disturbance
Installation	Backdoor & persistence, Lokikbot Trojan, Trickbot Trojan, AZORult Info stealer, Ransomware Samas, GradCrab

Aspects	Threats
Exploitation	RDP (Remote Desktop Protocol) brute force, Drive-by compromise
Delivery	Email phishing, SMS (short message service) phishing, fake testing apps, attacks against the teleworking infrastructure, attacks against health organizations, fraudulent domains: Corona-virus-map.com; Apps: COVID-19 tracker

In healthcare, incident reporting is a key process for the information technology (IT) department and depends on many factors. Clinical staffs carry mobile devices in most cases, have access to facility computers including email, and have access to programs that could threaten the very livelihood of the medical center community. Having a robust IT reporting system for incidents is a crucial function of the IT department. Clinical staff, ancillary staff, and management staff should have access to most incident reporting systems. In case of a threat such as phishing emails, Ransomware, or other malware from suspicious or malicious actors, the staff should be taught to report so IT staff can minimize the damage and halt any threat to patient care disruption.

II. Event/Incident Processing, Attacks Detection, and Threat Mitigation

Event prediction in big data forces the discovery and assimilation of interconnected techniques that focus on challenges, comprised of the following: 1) heterogeneous multi-output estimates [4], 2) complex needs amid prediction outputs [5], 3) a real-time run of prediction jobs) [6], and 4) trials in the big data event. The taxonomy of event prediction and related practices are shown in Table II [7].

Table II: Event Prediction and Techniques

Categorization (Goals)	Further Categorization (Output Forms of Goals)	Techniques
Location prediction	Point-based	● Unsupervised: spatial scan, network scan ● Supervised: spatial autoregressive, spatial multi-task learning, ● geo-featured classification
	Raster-based	● Trajectory destination prediction ● Spatial clustering, embedding, and convolution
Time prediction	Continuous time	● Survival analysis ● Point process ● Regression
	Discrete-time	● Indirect manner ● Direct manner
	Occurrence	● Anomaly detection ● (Auto-) regression ● Classification
Semantic prediction	Semantic sequence	Step 1: Event representation Step 2: Event causality inference Step 3: Future event inference
	Associate-based	● Frequent set mining ● Decision list
	Causality-based	● Whole-sequence classification: model-based, feature-based, prototype-based ● Next-event generation: descriptive-based, attributed-based

Joint prediction	Location and time	● Point-based: spatiotemporal point process, spatial temporal Gaussian process ● Raster-based: RNN, 3D CNN, CNN+RNN, spatial temporal CRF
	Semantic and time	● Time expression extraction ● Temporal association rule ● Multi-variate time-series forecasting
	Location, time, and semantics	● Tensor-decomposition-based methods ● Crowd wisdom-based methods: crowdsource systems, model ensembles ● Future event expression identification

It is important to the facility for IT staff to monitor specific functions of a potential attack. Programs in the cloud and the network are highly susceptible to malicious actors and events likely to become threats. In-depth-detection of an incident or event may be accomplished by employing one or more of the subsequent detection methods [8]:

- Network or cloud intrusion detection.
- Behavior monitoring—using machine learning, this function is an advanced correlation engine, and/or behavioral biometrics. It can be accomplished using the following techniques:
  - Service and infrastructure monitoring.
  - Network protocol analysis.
  - Network flow analysis.
- Privilege escalation detection—used to detect privilege escalation and these techniques embrace, but are not constrained to the following:
  - Host intrusion detection.
  - File integrity monitoring.
  - Attempted unauthorized user access detection.
  - Monitoring SaaS Services such as Office 365 or G Suite.
- Event correlation—gathering data from application logs or host logs and analyzing it to identify relationships and can be achieved using the following techniques:
  - Security incident and event management (SIEM).
  - Malicious host communication detection.
  - Using a centralized dashboard that selects threats based on user inputs.
- Physical security.

Threat mitigation is crucial to all enterprises, especially in hospitals. Greater risks and damage will occur very quickly without mitigation. Mitigation is a complicated issue and is related to current resources, available techniques or tools, and individuals with experience and skills. Basic cyber threats should be evaluated as to their severity. The simple methods of cybersecurity threat mitigation contain, but are not limited by the subsequent techniques [8]:

- Risk assessment
- Access control system
- Intrusion detection system
- Video surveillance system
- Policies and procedures
- Automated device data wiping—this technique uses tools that activate routine data wiping of departing employees' devices.

When Security Information and Events Management (SIEM) ends, Security Orchestration, Automation, and Response (SOAR) systems pick up the incident response procedure delivering an automated and arranged response during the Identification Phase, as well as the Containment, Eradication, and Recovery Phases. SOAR is a critical component of cybersecurity threat mitigation when disparate tools are integrated within a common platform. SOAR is a product line category of the Security Operations and Automation Platform Architecture (SOAPA). An

SOAPA platform puts together technologies through data collection, processing, analytics, and security operations. Table III describes an SOAPA system [9].

Table III: A Multi-Functional SOAPA System

Functions and Components	Description and Details
Data services functions	● Historical data ● Database management system (DBMS) ● Security logs ● Data loss prevention ● On premises & cloud-based services/ data, network traffic, etc. ● Other (network analyzers, alerts/ sensor systems, vulnerability scanners, honeypots/probes)
Security operations functions	● SIEM ● SOAR ● Intrusion detection system (IDS) ● Intrusion prevention system (IPS) ● Extended detection and response (XDR) ● Threat intelligence platform (TIP) ● Unified threat management (UTM)
Analytic functions	● Analytic AI/ML models
Integration functions	● Communication services ● Message/data formatting ● Processing ● Transformations
User interface & experience (UIX)/ Management Station	● User interface (UI) ● Security Operations Center (SOC) analysts ● Proactive SOAPA dashboard (notifications, alerts/events, attack predictions, and reporting)

Because AI/ML does not rely on static signatures utilized in conventional anti-virus systems, it is perfect for malware detection and anti-virus [10] [11]. Useful for finding and classifying phishing and malware emails, artificial neural network (ANN)-based models can [12] attain full AI/ ML empowerment of SOAR, and reinforcement learning (RL) models can be forced to control security orchestration, automation, and response. Autonomous software agents making observations and taking sequential actions optimally, with or without incomplete previous knowledge of the operational environment, can also be RL and consequently be predominantly flexible for deployment in real-time and dynamic cybersecurity environments [13].

III. Event and Incident Processing in Healthcare

Healthcare generally uses two kinds of event predictions: 1) individual-level for clinical longitudinal events and, 2) population-level disease outbreaks and epidemics. Extensive research on disease outbreaks for many different types of diseases and epidemics such as flu, H1N1, and COVID-19 has been conducted for population-level events [14]. Due to the rapid growth of massive surveillance data from government agencies, social media datasets, and other public datasets, a massive increase in the use of data-driven approaches to directly learn predictive mapping has developed [15]. Research has begun to focus on the individual level, including the longitudinal predictive analysis of individual health-related incidents such as adverse drug events [16] and sudden illnesses (e.g., strokes).

Incident reports can be submitted by physicians, providers, nurses, pharmacy technicians, biomedical equipment technicians, nursing assistants, administrative assistants, security guards, radiologic technologists, etc., depending on the specific situations of incidents, physicians, nurses, nursing assistants, radiologic technologists, biomedical equipment technicians, pharmacists, administrative assistants, security guards, etc. [1]. Yokohama City University Medical Center, Japan developed an incident reporting system. Anonymous, the incident reporting system included information about the incidents, like the professions, incident level, location, free-text content regarding the actual occurrence, and a measure to prevent future incidents. Currently, seven nationally defined incident levels exist in the system including Level 0—Incident with no direct impact on patients, Level 1—Incident with no substantial harm to patients, Level 2—Incident with only minor impairment to patient care requiring no further treatment, Level 3a—Substantial damage

to patients making it necessary to render further treatment to prevent a prolonged hospital stay, Level 3b—Significant damage to patient care models requiring further treatment including a prolonged hospital stay, Level 4—Permanent disability related to the accident, Level 5—Death related to accident. A Japanese hospital must report to the Japan Council for Quality Healthcare and publicly announce an incident that is Level 3b or above [17].

IV. Event and Incident Processing in a Large Medical Center

Charleston Regional Medical Center is a large medical center/hospital that serves patients in Mississippi, USA. In the Medical Center, events can be patient data theft, financial fraud, insurance fraud, password theft, personal health information theft, email phishing, etc. Ransomware occurrence, patient data theft, financial fraud, insurance fraud, personal health information theft, mobile device tampering, etc. are often treated as incidents. All incidents and events should be reported to the IT department, management, upper management, and risk management at first occurrence.

There are generally the following steps in the event/incident processing:

- *Event/Incident Detection:* At the first notice of a breach during patient care or management review of patient data or billing information.
- *Logging:* Need to be logged via a report in the IT department.
- *Categorization:* Categorized according to the level of incident severity and whether it will shut down patient care such as with Ransomware; for example, with Ransomware all patient care or billing is shut down by malicious actors with the intent to scam monetary reward for returning function. With a breach of patient data, this is categorized as a high priority because patient data is protected. Billing data is also protected.
- *Prioritization:* Low (e.g., email phishing); Medium (e.g., theft of passwords or medical equipment); and High (Ransomware, patient data theft, insurance fraud, billing fraud, etc.)
- *Response:* The police and IT departments need a detailed ongoing analysis and risk management program.
- *Escalation (Level 1, 2, or 3 Support):* Level 1 (such as email phishing and spam mail)—probably will not harm patient care; Level 2 (e.g., theft of medical equipment and mobile devices)—may shut down patient care; Level 3 (Ransomware, patient data theft, insurance fraud or billing fraud, etc.)—will shut down patient care.
- *Resolution/Recovery:* Will need to either pay the ransom or find a roundabout way to return patient care ability. Block email from personal accounts.

The Event and Incident Processing System is being implemented in the Medical Center to meet operational needs and improve cybersecurity. Annual training regarding event/incident processing and cybersecurity in healthcare is provided for all employees and contractors. The Event and Incident Processing System consists of the following components:

- *Data Services:* Network traffic, security logs, sensor systems, user behaviors, etc.
- *Big Data Analytics and AI/ML:* Data analytics, predictions, anomaly detection.
- *Dashboard/Display:* Events/incidents alerts or notifications.
- *Incidents/Security Reporting:* Internal/external reporting, agencies, third parties, and partners/collaborators.

V. Conclusion

Every incident is an event, although some events may not warrant an urgent reaction. As a result, incident reporting systems should be widely adopted for information collection regarding patient safety incidents. Most of the value for incident reports lies in the free-text section. In healthcare, incident reporting can be a critical function of the IT department and may depend on many factors. Clinical staff can carry mobile devices, have access to medical center

computers including email, and maintain access to programs that could threaten the very livelihood of the medical center community. A robust IT reporting system for incidents is a key function of the IT department. Clinical staff, ancillary staff, and management staff should have access to most incident reporting systems. In case of a threat such as phishing emails, Ransomware, or other malware from suspicious or malicious actors, the staff should be taught to report so IT staff can minimize the damage and halt any threat to patient care disruption. More hospitals are using big data in patient care. However, big data has many challenges and should be carefully considered by experts. Many hospitals are using AI in daily medical center functions. Using AI can alert the IT department of most threats before they become serious threats to halt all patient care functions. The IT department is using all manner of functions to identify threats and halt all threats to patient care before the threat becomes irreparable.

Acknowledgement

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

[1] H. Uematsu, M. Uemura, M. Kurihara, T. Umemura, M. Hiramatsu, F. Kitano, T. Fukami, and Y. Nagao, "Development of a novel scoring system to quantify the severity of incident reports: An exploratory research study," *Journal of Medical Systems*, vol. 46, no. 12, p. 106, 2022, doi: https://doi.org/10.1007/s10916-022-01893-1.

[2] G. Iakovakis, C.-G. Xarhoulacos, K. Giovas, and D. Gritzalis, "Analysis and classification of mitigation tools against cyberattacks in COVID-19 era," *Security and Communication Networks*, no. 1, p. 3187205, 2021, doi: https://doi.org/10.1155/2021/3187205.

[3] ENISA, ENISA Threat Landscape Report - 2020, 2021. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[4] N. Ramakrishnan, P. Butler, S. Muthiah, N. Self, R. Khandpur, P. Saraf, W. Wang *et al.,* "Beating the news' with EMBERS: Forecasting civil unrest using open source indicators," in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Minin*g, 2014, pp. 1799-1808.

[5] Y. Matsubara, Y. Sakurai, C. Faloutsos, T. Iwata, and M. Yoshikawa, "Fast mining and forecasting of complex time-stamped events," in *Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2012, pp. 271-279.

[6] F. Salfner, M. Lenk, and M. Malek, "A survey of online failure prediction methods," *ACM Computing Surveys (CSUR)*, vol. 42, no. 3, pp. 1-42, 2010, doi: https://doi.org/10.1145/1670679.167068.

[7] L. Zhao, "Event prediction in the big data era: A systematic survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1-37, 2021, doi: https://doi.org/10.1145/3450287.

[8] B. K. Schwab, "Insider threat management: Operating environments, detection methods and mitigation strategies," *Journal of Physical Security*, vol. 14, no. 1, pp. 13-34, 2021.

[9] J. Kinyua, and L. Awuah, "AI/ML in security orchestration, automation and response: Future research directions," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 527-545, 2021, doi: https://doi.org/10.32604/iasc.2021.016240.

[10] M. Berninger, and A. Sopan, "Reverse engineering the analyst: Building machine learning models for the SOC," 2018. [Online]. Available: https://www.fireeye.com/blog/threatresearch/2018/06/buildmachine-learning-models-for-the-soc.html

[11] D. Krisiloff, "Churning out machine learning models: Handling changes in model predictions," 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/churning-out-machine-learning-models-handling-changes-in-model-predictions.html

[12] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial intelligence in cyber threats intelligence," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, IEEE, 2018, pp. 1-4.

[13] M. H. Ling, K.-L. A. Yau, J. Qadir, G. S. Poh, and Q. Ni, "Application of reinforcement learning for security enhancement in cognitive radio networks," *Applied Soft Computing*, vol. 37, pp. 809-829, 2015. doi: https://doi.org/10.1016/j.asoc.2015.09.017.

[14] F. Petropoulos, and S. Makridakis, "Forecasting the novel coronavirus COVID-19," *PloS One*, vol. 15, no. 3, p. e0231236, 2020, doi: https://doi.org/10.1371/journal.pone.0231236.

[15] B. Adhikari, X. Xu, N. Ramakrishnan, and B. A. Prakash, "Epideep: Exploiting embeddings for epidemic forecasting," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 577-586.

[16] S. Santiso, A. Casillas, A. Pérez, M. Oronoz, and K. Gojenola, "Adverse drug event prediction combining shallow analysis and machine learning," in *Proceedings of the 5th International Workshop on Health Text Mining and Information Analysis (Louhi)*, 2014, pp. 85-89.

[17] T. Abe, H. Sato, and K. Nakamura, "Extracting Safety-II factors from an incident reporting system by text analysis," *Cureus*, vol. 14, no. 1, p. e21528, 2022, doi: https://doi.org/10.7759/cureus.21528.