Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN 1989 – 9572

DOI:10.47750/jett.2021.12.02.024

Evolving Beyond Patching: A Framework for Continuous Vulnerability Management

Jaipal Reddy Padamati[1]
Laxmi Sarat Chandra Nunnaguppala[2]
Karthik Kumar Sayyaparaju[3]

Journal for Educators, Teachers and Trainers, Vol. 12 (2)

https://jett.labosfor.com/

Date of reception: 20 March 2021

Date of revision: 19 June 2021

Date of acceptance: 18 September 2021

Jaipal Reddy Padamati , Laxmi Sarat Chandra Nunnaguppala, Karthik Kumar Sayyaparaju(2021).
Evolving Beyond Patching: A Framework for Continuous Vulnerability Management. ***Journal for Educators, Teachers and Trainers,*** **Vol. 12(2). 163 – .**

[1]Sr. Software Engineer, Comcast, Corinth, TX, USA, padamatijaipalreddy@gmail.com
[2]Sr. Security Engineer, Equifax Inc, Albany, NY, USA, sarat.nunnaguppala@gmail.com
[3]Sr. Solutions Consultant, Cloudera Inc, Atlanta, GA, USA, karthik.k.sayyaparaju@gmail.com

Journal for Educators, Teachers and Trainers
The LabOSfor electronic, peer-reviewed, open-access Magazine

Journal for Educators, Teachers and Trainers, Vol. 12 (2)
ISSN 1989 – 9572
https://jett.labosfor.com/

Evolving Beyond Patching: A Framework for Continuous Vulnerability Management

[1]Jaipal Reddy Padamati , [2]Laxmi Sarat Chandra Nunnaguppala, [3]Karthik Kumar Sayyaparaju
[1]Sr. Software Engineer, Comcast, Corinth, TX, USA, padamatijaipalreddy@gmail.com
[2]Sr. Security Engineer, Equifax Inc, Albany, NY, USA, sarat.nunnaguppala@gmail.com
[3]Sr. Solutions Consultant, Cloudera Inc, Atlanta, GA, USA, karthik.k.sayyaparaju@gmail.com

ADSTRACT
Having explored the key components of regulatory compliance in the cloud through the analysis of converge technology, this report advances to consider the significant elements of compliance through the application of Security Orchestration, Automation, and Response (SOAR), Security Information and Event Management (SIEM), and advanced threat detection measures. This paper's real-time and ground research-based simulation reports depict how these technologies are effectively utilizable and how strong security mechanisms can be established. Thirdly, the report also underlines the constant type of vulnerability management to extend the concept further compared to the regular patching work, highlighting vulnerability management as the consistent process to enhance an organization's readiness against threats and attacks continuously. The tasks and issues observed throughout implementation and the suggested strategies and recommendations are presented alongside illustrations and graphic visualizations. This paper presents an overview of compliance and security and their prospective for improvement within different organizations in the era of continually emerging threats.

Keywords: Regulatory compliance, Cloud computing, SOAR, SIEM, Threat detection, Vulnerability management, Resilience, Continuous assessment, Security posture, Patch management, Automation, Real-time scenarios, Simulation reports, Security frameworks, Proactive security, Risk mitigation, Data protection, Compliance strategies, Cybersecurity, Organizational security.

INTRODUCTION

In the present world dominated by the internet and computerization, cloud computing has emerged as the foundational element for organizations looking forward to improving their business performance and organizational facility capability in large measures. However, due to this development in recent years, which is the use of cloud services, complexities such as compliance with legal requirements and adequate measures have been brought out strongly. It regards compliance with laws, regulations, directives, requirements, and standards linked to the organization's business activities. Compliance in a cloud environment is not very easy because of the flexibility and distributed structures of cloud networks [1].

The purpose of this paper is thus to identify the approaches and tools that can be used to achieve compliance with cloud computing. Namely, emphasis is placed on applying security SOAR systems, SIEM systems, and sophisticated threat identification methodologies. Together, these technologies improve an organization's capacity to promptly identify, prevent, and address security threats, thus developing its security system [2].

SOAR is a security tool that combines many tools, and the incident response process is automated and, hence, faster. They enable a comprehensive evaluation of events and situations with correlated correlation data storage

and mechanism consolidation from different sources of information for SIEM systems. There is an understanding of machine learning and artificial intelligence methods applied to detect and counter advanced threats [3].

It means that detailed simulation reports and real-life situations will be provided in this report to let the audience understand how these technologies work in practice. Besides, it will explain the progressive approach to vulnerability management, underlining that vulnerability management should not be perceived as a one-time event focusing merely on patches. Thus, answering the challenges and suggesting solutions, this report is intended to contribute to a comprehensive understanding of the current trends and can serve as a guideline for organizations that rely on compliance and security improvements in the constantly changing environment.

Simulation Reports

Methodology

The simulation research that was conducted for this report was conducted in a bid to test the compliance of security technologies with the cloud computing environment. The methodology involved the following steps: These are the steps that were adopted in the course of the study:

Scenario Definition: First, it was necessary to identify present-day threats that organizational users of cloud services can meet. This was done by identifying standard attack types that included the following: 2 fake mail attacks, virus invasion, and distortion attempts. Thus, each scenario was designed to threaten specific aspects of the security technologies under consideration for integration. For example, the cases were applied in training to perform a legitimate analysis of violations, data breaches, insider threats, and compliance audits.

Tool Selection: The process that followed the formulation of the above goals was selecting the tools necessary for the simulation. This involved recommending Security Orchestration, Automation, and Response (SOAR) solutions, Security Information and Event Management (SIEM) solutions, and other advanced threat intelligence solutions. The selected tools were:

SOAR System: Phantom by Splunk because the approaches to security operations provided as containers allow for creating reusable plays, increasing the speed of response to security incidents [1].

SIEM System: Directions are allocated to IBM QRadar because it can support log management, threat analysis, and compliance tracking integration capabilities [2].

Advanced Threat Detection: CylancePROTECT is an artificial intelligence-based Endpoint Security solution that rose as the best solution to halt Advanced threats [3].

Simulation Setup: Preparing the context area was considered the most significant phase; the primary goal was to duplicate the environment as close to the cloud-only infrastructure as possible. These included establishing various levels of security, mainly the firewall, the intrusion detection system, and the multiple means of accessing control. The environment tried to be as authentic as possible, and this entailed the relative service models like IaaS, PaaS, and SaaS, as well as deployment models like the public clouds, private clouds, hybrid clouds, etc. Each was ready to record the events fitting the selected SIEM system for enhanced management and analysis.

Data Collection: Thus, during the simulation runs, data were captured in real-time to compare the effectiveness of numerous security technologies. This also included log files, alerts, and response times within the SOAR, SIEM, and threat detection systems. Therefore, the quantitative metrics discriminated into Key Performance Indicators were CTD, MTTD, MTTR, threat detection accuracy, and compliance report coverage. Regarding the data collection phase, we distinguished the elimination of false positives as well as the security threats of the system.

Tools Used

During these simulations, the following advanced instruments were employed, as stated below, because the following reasons that enhance the security operations and the legal necessities in the cloud:

SOAR Systems

Phantom by Splunk: Phantom was chosen, as it represented solutions for the security operation and management of the response scheme. This tool should assist the security team in reducing the mean time to respond (MTTR) as most repeated

processes are automated. Thanks to actioning many security tools and security systems, Phantom can accomplish the playbooks for incidents and responses; therefore, it does not take human analysts' time to complete simple operations. The creation of the Phantom ensured that it was set to be active in conducting pseudos foreseen security threats such as the wrong attempts at getting access to a computer or other gadgets and viruses that tend to intrude into the system; actions to be taken include isolation of the affected computer and other related gadgets, informing the security department and not least, being able to produce records of the entire episode for auditing purposes. From the above-described application of Phantom, it can be concluded that Phantom's performance regarding the working response time was rather splendid; thus, integrating this method into the security plan is crucial [1].

SIEM Systems

IBM QRadar: Originally, IBM QRadar was adopted mainly because of functions such as log and threat analysis and compliance. As an SIEM system, QRadar aggregates the log, events, and all relevant information about the cloud systems presented in this paper. They work with data from various sources comprising structures in the network, servers, and applications and search for discrepancies that may indicate threats. In the simulations, QRadar was the system that had to gather the log data and events, the latter being patterns that suggested a security threat occurrence; on the same note, QRadar was to send notifications. Moreover, compliance reporting in QRadar was employed to produce reports that implied that the company was compliant with the obligation of the laws. As security is always the prime concern of any organization, the live representation of the tool in handling the cloud environment's security has helped detect the threats and eliminate them on the spot [2].

Advanced Threat Detection

CylancePROTECT: For endpoint protection, CylancePROTECT, an AI-powered endpoint security solution, was used because of its high anti-threat efficiency. It is dissimilar to other terminal point-end signature-based antivirus software programs, which use machine learning methods to analyze the information of behaviors and then shut down the associated dangerous activities. It also permits the detection of new and growing threats, which the other systems that rely on signature cannot identify. During the simulations, CylancePROTECT was deployed on various endpoints in the company's cloud system to mitigate or eradicate malicious activities or indications early. The different attack scenarios were simulated to evaluate its capability to detect complicated threats like the zero-day exploit kits and the complicated latent threats or APTs. The result depicted that the CylancePROTECT reduces the chances of successful cyber attacks and enhances the security condition of the cloud system [3].

Altogether, these tools protected various tiers within the field of security management, from handling specific incidents and log analysis to detecting the highest threat classes. These simulations proved that the best security strategy is the layered one, which includes the positive aspects of all those technologies.

Results Obtained

The results of the simulations provided valuable insights into the performance of the security technologies. From the simulation outcomes, the performance of the security technologies was as follows evident:

SOAR System Performance

Implementation and Impact: In fact, the employment of Phantom also helped to cut down the MTTR to a considerable extent. Of all the options, the realization of repetitive tasks such as event categorization, prioritization, and subsequent escalation appeared to have the most significant potential since they reconsidered the priorities of the security teams and left them more time for essentials. It also improved the speed of responding to the incidents at the exact time, conformity of the process, and effectiveness in handling the occurrences. For instance, when many alerts went off simultaneously, Phantom could correlate such alerts and execute tasks that entail running scripts containing the infected systems, informing the relevant parties, and initiating investigation processes. It was crucial, thus, to have such a simple and swift response mechanism to limit the consequences of security breaches where there was proof of Phantom's role in enhancing productivity and orderliness[1].

Workflow Orchestration: For that reason, Phantom's ability to oversee the coordinated and concurrent operation of multiple tiers between the different security tools seemed helpful in this regard. The simulations involved preparing how Phantom might interact with the organization's other systems: firewall, EPP, and SIEM. These and such other coordination and synchronization made it possible for the different elements in the security solution to mesh well with each other; thus, there was no strand left when dealing with threats. For instance, in a specifically artificial ransomware attack, Phantom realized that the potential attack phase was opened and initiated isolation procedures for the affected systems and backup restoration at a time equal to a few minutes. There is no doubt that the various stakeholders responded in an efficient and coordinated manner to reduce the time for which the system was unavailable. In actualizing this, the least amount of data was lost as well.

SIEM System Effectiveness

Real-time Detection and Analysis: The first one focused on the fact that the various functions of IBM QRadar pointed to the analysis and identification of security incidents in the different cloud structures. The centralized logging and real-time analysis allowed us to identify the violations of compliance and security threats immediately. The integration of QRadar

in the network opened multiple logs from the security tools, making it possible to determine the nature of the attack and its various patterns. During the simulations of the security threats, it was possible to observe that QRadar can detect and further report threats such as unauthorized access, data leaks, and a rise in privileges. The security administration stated that the system highly appreciated the real-time portrayal of security in the cloud milieu, which helped to manage the threats that have been identified and responded to in actual time [38].

Compliance Reporting: Twelve, an earlier discussion considered one of the product strengths discovered concerning QRadar: the adherence reporting feature. Also, all these types of reports can be personalized in this system, and the templates this system contains serve to create compliance reports, which would show how compliance is done to the requirements. In these cases, GDPR, HIPAA, and PCI-DSS regulations were addressed with the help of QRadar, which provided corresponding reports. Such reports also contained information on security events, time consumed on investigations and their solutions, compliance details, and many others, providing no doubts about the organization's security condition. Specifically, this capability was useful in audits, especially when an organization had to provide evidence of compliance with a particular standard to the authorities or investors.

Advanced Threat Detection

AI-driven Threat Mitigation: Notably, it was evident that CylancePROTECT discerned and responded to such threats that modern signature-based AV clients could not even register. Once more, the CylancePROTECT AI solution effectively eliminated threats, including malware and numerous APTs, before they infiltrated the organization's network. However, they argued that it would be challenging to set them up without a high level of mathematical skill. CylancePROTECT was able to recognize several types of activities that were malicious but did not fit any of the predetermined standard patterns of the signatures. This future threat recognition ability was illustrated especially during the exercises using zero-day exploits and polymorphic viruses, and all of them were detected and eradicated by CylancePROTECT before they could cause any harm [3].

Behavioral Analysis: Frank also saw that CylancePROTECT detected advanced threats proactively better than CrowdStrike, besides the deep behavioral analysis that CylancePROTECT performed. In the simulation, I observed the activities of the applications and processes on the platform. I paid attention to the changes in the files, network connections, and resources, which can be signs of compromise. If an event triggered the suspicion, the program immediately isolated the endpoints, thereby effectively stopping the malware propagation and providing an endpoint report. More so to the behavioral analysis approach, this proved pertinent in insider threat scenarios where the given activities were not implicitly clear through the systems and controls.

REAL-TIME SCENARIOS

Scenario 1: Possible Intrusion Attempt

The attacker employs a tactic of password cracking to infiltrate since employees are likely to have made a weak password. Once they have entered, the attacker attempts to gain more privileged access to essential information. ***Relation to Simulations:*** In the Simulation, the IBM QRadar SIEM system's configuration included data analysis for any outliers in the login traffic and signs of brute-force patterns. When failed login attempts were observed, QRadar produced an alert and forwarded the information to the Phantom SOAR system, specifically if consecutive failed attempts were made. A response playbook in Phantom was activated immediately, and the actions involved blocking the IP used by the attacker, escalating it to the security team, and recording the activity for compliance purposes. This was a real-time counterpart of what had occurred during the simulated cases in which an unauthorized access attempt was flagged and neutralized immediately [1].

Scenario 2: Phishing Attack

An employee gets an email that resembles an authentic message sent by a reliable organization, person, or company. The context of the received email message is a link that, when accessed, infests the employee's working station with malware. The malware then tries to move to another computer in the network to gain access to essential equipment and information.

Relation to Simulations: The results of the simulations were compared with those of the other solutions capable of preventing the given kind of phishing attacks based on machine learning algorithms used in CylancePROTECT. When the link with the virus was found, the CylancePROTECT application did not allow the link to be followed and, therefore, prevented the execution of the malware. Moreover, Phantom was set up so that it could also perform a response by containing the infected workstation and alerting the incident response team. The real-time scenario clearly showed how CylancePROTECT prevents malware execution and Phantom in managing a complete reaction [2].

Scenario 3: Data Exfiltration

A legitimate system user tries to steal organizational data by copying files and uploading them to another server. The insider employs unnoticeable communication vectors so as not to be captured by conventional security mechanisms. **Relation to Simulations:** In the simulations, the system was configured so that IBM QRadar would follow data transfer

activities and identify other abnormal activities, such as transferring large files to external IP addresses. When the data exfiltration attempt was identified, QRadar sent an alert and called in Phantom to intervene. Thus, Phantom's plan contains three elements: stopping the data transfer, denying insider access, and conducting a data loss assessment to determine the full scale of the problem. Such a case demonstrated how QRadar could identify the malicious movement of data and how Phantom could manage the response [3].

Scenario 4: Ransomware Attack

Ransomware attacks the organization's cloud environment, locks essential files, and asks for a decryption code in exchange for payment. The moves blanket the environment, embracing more systems and paralyzing organizational activities.

Relation to Simulations: Concerning the simulated scenarios in the test, CylancePROTECT's ability to prevent ransomware attacks was as follows. The CylancePROTECT tool was able to detect and prevent the ransomware from being able to encrypt files on the computer. Moreover, Phantom helped to automate the response process effectively; the organization isolated sick computers, launched backups, and informed the users. This real-time use case explained how CylancePROTECT stopped the ransomware from running, and Phantom mitigated the impact to reduce business disruption [4].

Scenario 5: Compliance Audit

An organization inspection is conducted secretly by the regulatory body to check compliance with data protection laws. The auditors are likely to seek special reports on incidents, their handling time, and other security and compliance activities undertaken by the organization.

Relation to Simulations: While performing the simulations, IBM QRadar's functions in creating compliance reports regarding the company's conformity to the guidelines were employed to prepare comprehensive reports showing compliance with the set regulations. QRadar gathered sufficient information in record time and generated concise compliance reports in another live situation. Phantom could automatically create a collection of essential logs and documents, which helped the organization prepare for the audit. This situation highlighted the need for proper compliance reporting instruments and specific mechanisms to carry out an audit [5].

Graphs

Simulation Data Tables

Table 1: Unauthorized Access Attempts

Time (hrs)	Unauthorized Access Attempts
1	10
2	15
3	8
4	20
5	25

Table 2: Phishing Emails Detected

Time (hrs)	Phishing Emails Detected
1	5
2	8
3	12
4	10
5	15

Table 3: Data Exfiltration Attempts

Time (hrs)	Data Exfiltration Attempts
1	2
2	4
3	3
4	5
5	6

Table 4: Ransomware Incidents Prevented

Time (hrs)	Ransomware Incidents Prevented
1	1
2	3
3	2
4	4
5	5

Table 5: Compliance Audits

Compliance Audits	Compliance Score (%)
Audit 1	85
Audit 2	90
Audit 3	78
Audit 4	88
Audit 5	92

Challenges and Solutions

Challenge 1: Coordination in the integration of miscellaneous security devices. While doing the research and the simulations, one of the main scenarios explained was security tools interoperation. As for the configurations of the systems, data, and workflows, SOAR, SIEM, and advanced threat detection systems are distinct. However, ensuring interoperability and the security of the tools presented a significant challenge in the process.

Solution: To avoid this, the standard mechanism based on the refined API and data format presented itself as the solution. For instance, Phantom software by Splunk uses RESTFul API to communicate with other security gadgets regarding data sharing and subsequent organization of the security process [1]. Moreover, I mentioned the following advantages regarding the decision to select the modular architecture in which every aspect of IT security could be modified without affecting the other segments. Adequate tests were performed periodically and at the integration points, thus ensuring the integration of the information flows.

Challenge 2: Special Cases of Processing Large Quantities of Security Information

The fourth major issue that online networking raised was how to manage a massive amount of security data generated by the cloud structure. For instance, in the case of the SIEM system, there was the requirement to process log data in real time, and thus, an adequate number of CPU and data processing mechanisms were required.

Solution: This was achieved by applying data preprocessing techniques and hosting ample cloud resources to deal with this issue. For example, IBM QRadar uses data analytics and machine learning techniques to go through the large amount of data. Instead of showing the user all the data, it only shows the one crucial to security [2]. That is why approaches such as serverless computing and distributed data processing were helpful in the project as they helped scale it and process the data.

Challenge 3: These are the most significant challenges that must be overcome to improve the ability to identify and effectively counter contemporary threats.

New-generation threats such as the zero-day attacks and the APT constitute a significant threat given how they are developed. For these threats, real-time detection and response add more pressure to the IDS and IPS solutions, and the reaction means.

Solution: Rather, fresh AI-based threat identification solutions like CylancePROTECT were employed to enhance the identification of more complex threats. CylancePROTECT uses machine learning algorithms that are trained with large volumes of known and unknown threats on what is referred to as behavior-based learning rather than pattern-based, assuming that it will be able to detect the attack behavior from the learned patterns [3]. It does so to detect unknown threats like the zero-day attack and APT before they cause significant losses. Moreover, synchronizing with Phantom, additional deeper integration suggested opportunities to add reaction actions that, for example, would include CylancePROTECT and such measures as isolation of the compromised systems and beginning the investigation of the advanced threats.

Challenge 4: About the Management of the Laws and Codes of Business. Sticking to several compliance standards, especially in the current cloudy environment, was another challenge. Now and then, it was almost possible not to observe

compliance with OFAC's regulations because compliance was complex with the constantly evolving standards and framework in the US.

Solution: Therefore, complex CM features employed in the SIEM systems, including the IBM QRadar, were used to solve this problem. Therefore, as peras to multiple templates that are ready to be incorporated in various kinds of reports, with innovative adoptions and particularized reports, compliance reports were relatively easy to create in QRadar [2]. The integration of the ongoing compliance check mechanisms through the SOAR meant that there were always checks and balances regarding the status and any changes of the compliance status and other instances of noncompliance. Also, the practices adopted in reviewing and updating the security policies to meet the legal requirements set out served as a way of checking compliance.

Challenge 5: Those Related to the False Positives and False Negatives. False positives and negatives are the occurrences of alerting to a threat when there is no one and failing to identify an existing threat. Of concern was the typical question of how to achieve high sensitivity and, at the same time, maintain specificity to reduce the occurrence of such as much as possible.

Solution: Other changes introduced to the detection process, such as SIEM and threat detection, involved changing the algorithms used in the detection process and the correlation rules used in the system to reduce false positives/negatives. There were machine learning models in CylancePROTECT, and new info fed the models to make them more accurate [3]. Moreover, topics such as multi-factor authentication and multi-layer security controls were also found to help add validation layers. Hence, the system will discover sounding a false alert is almost impossible. Regular activities and otherwise suspicious activity from the UBA embedded in the preceding SIEM system also helped eradicate other false positive cases.

From the above challenges, it is pretty clear that running a secure and compliant cloud is not a walk in the park, as the solutions above suggested suggest. Thus, it is stated that by applying technologies and ensuring that the organization is comprehensive and approaches the problems and risks actively and inclusively, the challenges mentioned above can be eliminated, and the organization's security posture can be enhanced.

Conclusion

This paper has looked at the critical survival issues and measures that are very useful in establishing and achieving secure regulatory cloud computing about security model, Security Orchestration, Automation, and Response (SOAR), Security Information and Event Management (SIEM), and the other advanced threat detection system specialized in the formation of the team security model.

Key Findings

Effectiveness of SOAR Systems:

Therefore, introducing the ideal SOAR systems into an organization, such as Phantom by Splunk, has made it possible to have less Mean Time to Respond to security threats. Phantom enabled task automation and appropriate management of numerous relations connecting people, tools, and systems, which allowed to minimize the time needed to respond to security incidents and, therefore, to reduce the consequences of cyber-attacks [1].

Capabilities of SIEM Systems:

Regarding the substantially realized performances, it was identified that security event detection and analysis in real-time was well implemented in IBM QRadar. Specifically, the firm was impressed by its log management, threat detection, and compliance reporting features that would make the cloud system more secure and CPE compliant. Particularly regarding compliance requirements, using additional sources, linking the data with other systems, and automatically generating exceptional compliance reports were important [2].

Advanced Threat Detection:

Studies conducted on CylancePROTECT demonstrated the favorable self-learning outcomes achieved when identifying new threats and their prevention, as well as APT and zero-day threats. Hence, threat detection was not based on signatures but was preventive by employing machine learning models of behavioral interactions [3].

Continuous Vulnerability Management:

This was being fueled by new threats that could not be tackled through a steady patching process, making vulnerability management a key factor. This ensured that cases of the opponent resulting in exploitable opportunities were eradicated because continuing vulnerability assessments were performed ceaselessly to ensure compliance and security were maintained [1][3].

Implications

Therefore, the recommendation that can be seen from this report is that there should be a notion that cuts across organizations to adopt an overall approach to cloud security and compliance. There is a protection plan comprising SOAR, SIEM, and the advanced threat detection system that enhances protection, sometimes called security posturing, which improves the identification of security threats and manages to counteract or contain them. Hence, when such technologies are deployed, the organizations can put in place stricter measures and maintain compliance to the legal provisions and therefore guarantee the protection of sensitive data while simultaneously guaranteeing organizational legitimacy to their stakeholders.

Also, threat and opportunity identification is constant, and using sophisticated threat identification, AI provides a better chance for the organization to be prepared to fight off cyber threats. Besides raising the general level of organizational operational efficiency, this approach also ensures the regularity of compliance, thus reducing the organizational vulnerability to legal sanctions and negative stereotyping.

Hence, properly integrating these advanced security solutions and practices is necessary to manifest in organizations that intend to handle various challenges relating to cloud computing and guarantee adequate security measures. Thus, the continuous enhancements of these technologies will be crucial in the future, providing a safe cloud platform.

References

1"Phantom: Security Orchestration and Automation," Splunk, 2020. [Online]. Available: https://www.splunk.com/en_us/investor-relations/events.html.

2"IBM QRadar: Security Information and Event Management," IBM, 2019. [Online]. Available: https://www.ibm.com/security/security-information-and-event-management.

3"CylancePROTECT: AI-Driven Endpoint Protection," Cylance, 2018. [Online]. Available: https://www.cylance.com/en-us/products/cylanceprotect.html.

4 M. A. Khan and Q. H. Malluhi, "Establishing trust in cloud computing," *IT Professional*, vol. 12, no. 5, pp. 20-27, 2010.

5 T. Sommestad, M. Ekstedt, and P. Johnson, "A probabilistic relational model for security risk analysis," *Computers & Security*, vol. 29, no. 6, pp. 659-679, 2010.

6 E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, p. 80, 2011.