Using SIEM and SOAR for Real-Time Cybersecurity Operations in Oil and Gas

Suchismita Chatterjee

Texas, U.S.A
suchi5978@gmail.com

Abstract

The oil and gas industry is a prime target for cyberattacks due to the critical infrastructure it controls and the high value of its data. This paper explores the evolving landscape of cyber threats facing the industry, including sophisticated attacks, ransomware, DDoS attacks, phishing, and insider threats. It delves into the challenges posed by the convergence of IT and OT systems, ICS vulnerabilities, supply chain attacks, and legacy systems.

To address these threats, the paper examines the role of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) technologies. SIEM provides real-time monitoring and analysis of security events, while SOAR automates incident response and reduces mean time to resolution (MTTR) and mean time to detection (MTTD). The paper discusses how SIEM and SOAR can be used together to enhance threat detection, response, and proactive threat hunting.

Furthermore, the paper explores the benefits and limitations of SIEM and SOAR, including cost, complexity, and skillset requirements. It provides best practices for implementing these technologies, such as establishing clear security policies, implementing a layered security approach, and regularly updating security rules and playbooks. By leveraging SIEM and SOAR, oil and gas companies can significantly improve their cybersecurity posture and protect their critical infrastructure and sensitive data.

Keywords: Cybersecurity, Oil and Gas Industry, Cyber Threats, Ransomware, DDoS Attacks, Phishing, Insider Threats, IT and OT Security, SIEM, SOAR, Security Orchestration, Automation, Response, Threat Detection, Incident Response, Cyber Risk Management, Critical Infrastructure Protection, Cybersecurity Best Practices

I. INTRODUCTION

The oil and gas industry faces a constantly evolving landscape of cyber threats. From sophisticated state-sponsored attacks to financially motivated ransomware attacks, the industry must be prepared to defend its critical infrastructure and sensitive data. Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) are two technologies that can play a crucial role in real-time cybersecurity operations for oil and gas companies.

The oil and gas industry is a prime target for cyberattacks due to the high value of the data and systems they control, the potential for disruption to critical infrastructure, and the economic and societal impact of such disruptions[2]. Attacks are becoming more frequent and more sophisticated.[3] Most oil and gas companies look at five areas of risk related to cyberattacks: financial, reputational, impact on people and safety, damage to assets, and effects on the environment.[4]

Some of the most common cyber threats targeting IT systems in the oil and gas industry include:

- **Sophisticated Cyber Threats:** These can originate with state-sponsored actors, hacktivists, and criminal syndicates. Nation-state-backed cybercriminals are increasingly using AI-powered tactics like targeted phishing and automated vulnerability exploitation to cause maximum disruption.[5]
- **Ransomware:** Cybercriminals regularly target workers with deceptive emails (i.e., phishing), compromising their credentials or tricking them into installing malware.[5]
- **Distributed Denial of Service (DDoS) Attacks:** Networks can be overwhelmed by a large-scale distributed denial of service (DDoS) attack, leading to service disruptions.[1]
- **Phishing Attacks:** Phishing attacks are often used to deliver malware or steal credentials, which can then be used to launch further attacks.

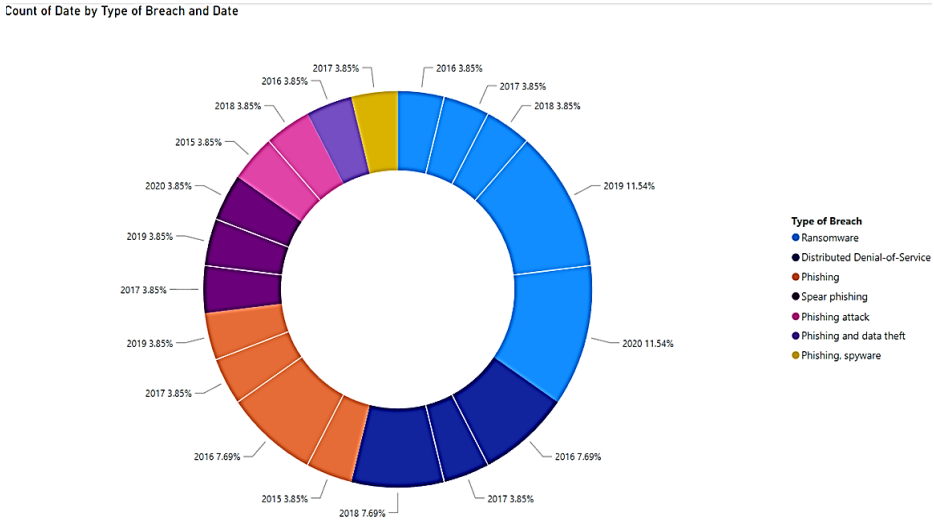

Figure 1: Prominent cyber threats targeting IT systems in the oil and gas industry

Operational technology (OT) systems, including distributed control systems (DCS) and supervisory control and data acquisition (SCADA), are also susceptible to cyber threats. While OT systems may be more difficult to hack directly, attacks often originate on the IT side and then move laterally into the OT environment. Key challenges in securing OT environments include:

IT and OT System Integration: The increasing convergence of IT and OT systems in the oil and gas industry improves efficiency but also creates new cyberattack vectors. This convergence requires integrated security solutions that can protect both IT and OT environments.

ICS Vulnerabilities: ICS vulnerabilities can be exploited to disrupt operations, cause physical damage, or even create safety and environmental hazards.

Supply Chain Attacks: A supply chain attack on an oil and gas company is a cyberattack that targets the company's suppliers, vendors, or other partners to gain access to the company's systems and sensitive information. Oil and gas professionals rank inadequate oversight of the vulnerabilities of supply chain partners connected to their organization's environment as the greatest challenge in enhancing OT cybersecurity.[6,4]

Legacy Systems: The oil and gas sector uses many legacy systems that lack the strong security measures to combat modern threats. These systems often run on obsolete operating systems that no longer receive security updates, making them prime targets for cyberattacks such as data breaches and ransomware.

Disgruntled employees, particularly those with access to sensitive data and systems, can cause severe damage if they choose to misuse their privileges.[2]

The consequences of these attacks can be severe, including:

- **Financial losses:** Ransomware attacks can result in significant financial losses, with recovery costs averaging US$3.12 million per incident.[5]
- **Reputational damage:** Cyberattacks can damage a company's reputation and erode customer trust.[4]
- **Disruption of operations:** Attacks can disrupt operations, leading to production downtime and lost revenue.
- **Safety and environmental risks:** Attacks on ICS can have safety and environmental consequences, potentially leading to equipment damage, leaks, or spills.

Furthermore, independent oil and gas companies often face unique challenges, such as outdated software, limited employee training, and a lack of a coherent incident response plan. [7]These challenges can make them more vulnerable to cyberattacks compared to larger players in the industry.

II. How SIEM and SOAR Can Help

SIEM and SOAR are two powerful tools that can help oil and gas companies address these cybersecurity threats.

- SIEM (Security Information and Event Management)

SIEM platforms provide deep insights into potential cyber threats by aggregating and analyzing security data from various sources. SIEM's primary function is to:

- Collect data: SIEM collects security event data from various sources across the IT environment, including network devices, servers, databases, and security appliances. Modern SIEM solutions can ingest data well beyond traditional security logs from network and cloud, along with data from containers, commercial off-the-shelf software (COTS) and non-COTS applications, system configurations, and more.[10]
- Analyze data: SIEM normalizes, aggregates, and displays the collected data in one pane of glass for security teams to gain insights into activities. It uses advanced algorithms to detect anomalies and generate alerts when it finds unusual patterns.[11]
- Identify threats: Paired with detection rules, either pre-built or self-managed, SIEM detects anomalous behavior that indicates potential compromise or exploitation that can lead to security breaches. Next-generation SIEM solutions have integrated threat hunting capabilities, allowing analysts to uncover suspicious activity alerting the security team when it detects suspicious activity.[9,10]
- Detecting backdoors and dormant threat actors: SIEM can be used to detect backdoors in systems and identify dormant threat actors.

SOAR (Security Orchestration, Automation, and Response)

- SOAR technologies lie further downstream from SIEM's log ingestion, providing automated analysis that aims to rapidly prioritize and respond to flagged security incidents. SOAR's primary function is to:[8]

- Gather data: SOAR gathers data from various sources, including SIEM, threat intelligence platforms, and other security tools.
- Prioritize alerts: SOAR prioritizes alerts based on threat levels. This can include automated alert assignment to optimize the distribution of alerts and incidents among security analysts.[14]
- Automate responses: SOAR automates responses to a wide range of threats based on predefined workflows. This is known as a triggered outcome. Once a threat is identified, SOAR can automatically take action, such as isolating infected systems or blocking malicious IP addresses.[11]
- Reduce MTTR and MTTD: SOAR helps reduce the mean time to resolution (MTTR) and mean time to detection (MTTD) of security incidents.

III. How SIEM and SOAR Work Together

SIEM and SOAR work together to enhance security operations (SecOps) by:

- Enhanced threat detection and response: SIEM monitors security data in real-time to identify potential threats, and SOAR automates the response to those threats.
- Streamlined data integration: When SIEM and SOAR are combined, alerts and incident data move together smoothly, giving security teams a full picture of incidents.
- Automated incident handling: SIEM alerts notify SOAR's playbooks what to do in reaction, like isolating systems or blocking IP addresses.
- Proactive threat hunting: SIEM and SOAR can be used together for proactive threat hunting, leveraging threat intelligence, anomaly detection, and automated response playbooks to identify and mitigate threats before they can cause damage.

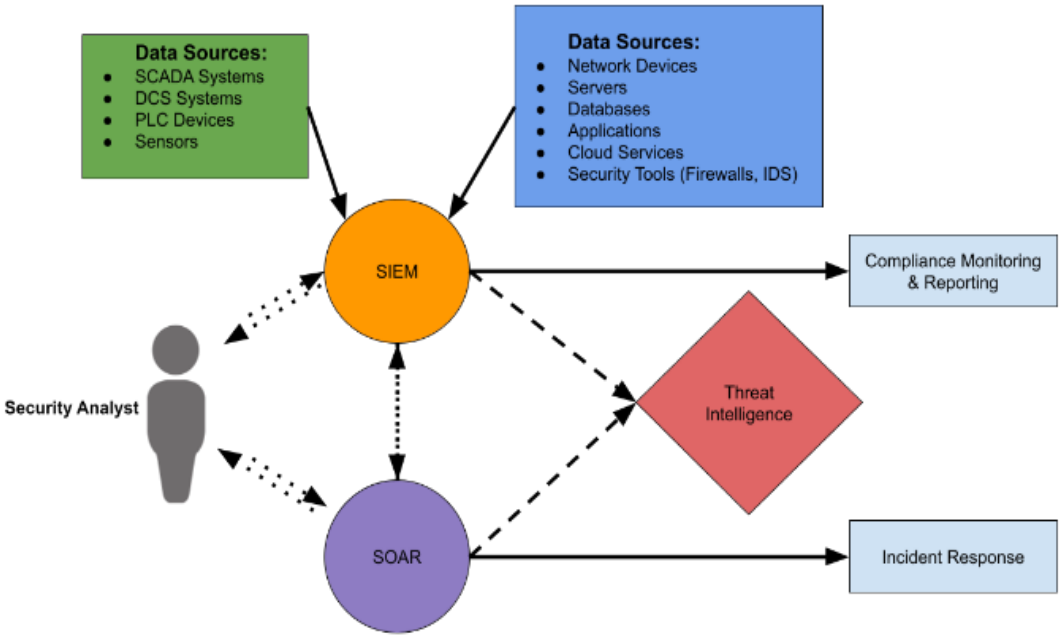

Figure 2: Relation between SIEM and SOAR

Threat	SIEM Capabilities	SOAR Capabilities
Ransomware Attacks	Detects malicious activity, such as unusual file access or modification. Helps identify the source of the attack and the extent of the damage. Provides real-time monitoring and analysis of security events to detect ransomware activity early on.	Automates the containment of ransomware attacks by isolating infected endpoints, terminating malicious processes, and blocking known malicious IP addresses and domains.
Phishing Attacks	Analyzes firewall, IDS, and IPS logs against threat feeds to alert you if a request is coming from a malicious URL.	Automates phishing investigation and response by pulling suspected phishing emails from the inbox, blocking malicious URLs and attachments, and resetting passwords for compromised accounts.
DDoS Attacks	Monitors web server logs and flags anomalous traffic events that may be indicative of a DDoS attack.	Can automate DDoS mitigation strategies such as rate limiting, IP filtering, and blackholing.
Insider Threats	Detects unusual user activity, such as accessing sensitive files or attempting to escalate privileges.	Automates the response to insider threats by disabling user accounts, blocking access to sensitive data, and alerting security teams.
Supply Chain Attacks	Monitors network traffic for suspicious activity originating from third-party vendors or suppliers.	Automates the response to supply chain attacks by blocking traffic from compromised vendors, isolating affected systems, and inciting incident response procedures.

Table 1: Capabilities of SIEM and SOAR

IV. BENEFITS AND LIMITATIONS OF SIEM AND SOAR

Systems in oil and gas operations presents unique security challenges, requiring specialized solutions to protect critical infrastructure and sensitive data. Furthermore, the oil and gas industry has experienced an uptick in cyberattacks in recent years, making robust cybersecurity measures essential. In response to this growing threat, many oil and gas companies have adopted security information and event management (SIEM) and security orchestration, automation, and response (SOAR) technologies to enhance their cybersecurityposture.

SIEM technology helps organizations collect, analyse, and monitor security events from various sources in real-time to identify and respond to potential threats. SIEM solutions offer several benefits to the oil and gas industry, including:

- Enhanced Threat Detection: SIEM solutions improve the ability to detect complex and sophisticated cyber threats by correlating security events from different sources and identifying patterns that may indicate malicious activity. In the oil and gas industry, where even minor disruptions can have significant consequences, real-time threat detection is critical. SIEM can help identify threats such as pipeline sabotage, attempts to disrupt refinery safety systems, or data breaches that could expose sensitive operational data.

- Improved Incident Response: SIEM solutions enable faster and more effective responses to security incidents by providing real-time alerts and automated response actions. By consolidating security events and streamlining alert management, SIEM helps reduce alert fatigue and ensures that security teams can focus on the most critical threats. For example, a SIEM solution could quickly identify and alert on unauthorized access attempts to critical systems, allowing security teams to take immediate action to contain the threat.

- Faster Detection and Response: The ability to provide faster detection of and response to security events is a crucial benefit of SIEM. In the oil and gas industry, where operational continuity is paramount, rapid response to security incidents can prevent disruptions to production, protect critical infrastructure, and minimize financial losses.

- Better Visibility into Threats: SIEM solutions provide better visibility into threats by aggregating and analyzing security data from various sources. This enhanced visibility allows security teams to gain a comprehensive understanding of the threat landscape and identify potential vulnerabilities in their systems. For instance, a SIEM can help identify patterns of suspicious activity that may indicate an ongoing attack campaign targeting the organization's oil and gas facilities.

- More Efficient Security Operations: SIEM solutions contribute to more efficient security operations by automating tasks such as log collection, analysis, and reporting. This automation frees up security personnel to focus on more strategic initiatives, such as threat hunting and vulnerability management, improving the overall efficiency of security operations.

- Compliance Management: SIEM solutions simplify the process of meeting regulatory requirements and preparing for audits by providing pre-built reports and dashboards oriented around compliance. For example, SIEM can help oil and gas companies comply with regulations such as the North

American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards by providing real-time monitoring and reporting capabilities.

- Centralized Security Management: SIEM solutions provide a single pane of glass for monitoring and managing security across the entire IT infrastructure. This centralized view allows security teams to efficiently monitor and manage security events, identify potential threats, and respond to incidents in a coordinated manner.

- Operational Efficiency: SIEM solutions streamline security operations and reduce manual effort by automating tasks such as log collection, analysis, and reporting. This automation frees up security personnel to focus on more strategic initiatives, such as threat hunting and vulnerability management, improving the overall efficiency of security operations.

- Benefits for Managed Service Providers (MSPs): SIEM tools can be particularly beneficial for MSPs serving oil and gas clients. They provide simplified compliance reporting, greater visibility into IT environments, and scalability to support the growing needs of clients. This allows MSPs to offer enhanced cybersecurity services to their oil and gas clients, helping them protect their critical assets and maintain operational continuity.

- Supply Chain Security: The interconnected nature of the oil and gas industry introduces weaknesses through third-party vendors and suppliers. SIEM solutions can help mitigate supply chain risks by monitoring activity in networks and regulating access to industrial assets, both in the field and out of the field. This helps prevent unauthorized or malicious access from third-party vendors and protects critical infrastructure.

- Addressing Challenges for SMEs: Small and Medium Enterprises (SMEs) in the oil and gas sector often face challenges such as budgetary constraints and lack of cybersecurity expertise. SIEM solutions can help SMEs overcome these challenges by providing cost-effective security monitoring and threat detection capabilities.

Despite these benefits, SIEM solutions also have limitations, such as:

- Configuration Complexity: Configuring a SIEM system to meet the specific needs of an organization can be complex and time-consuming, requiring specialized expertise and careful planning. The complexity of configuring SIEM solutions can lead to misconfigurations and gaps in security monitoring, potentially allowing attackers to exploit vulnerabilities.

- Integration Challenges: Integrating SIEM tools with existing security tools and legacy systems can be challenging due to compatibility issues, potentially hindering the SIEM's ability to provide a complete view of security events.

- Resource Intensive: SIEM implementation requires a significant investment of time, money, and skilled personnel, which can be a barrier for smaller organizations with limited budgets. The high cost of SIEM solutions can be a barrier for smaller oil and gas companies, limiting their ability to implement comprehensive security monitoring1.

- Hidden Costs: The hidden costs of SIEM, such as those associated with data storage, maintenance, and upgrades, can strain budgets and disrupt the SIEM implementation process.

- Data Onboarding: Ensuring that all relevant data sources are properly onboarded into the SIEM system can be challenging due to different log formats and data structures, potentially compromising the SIEM's effectiveness in threat detection.

- Scalability: Organizations need SIEM solutions that can scale with their growing data volumes and security needs, which can be a challenge for some SIEM solutions.

- Data Retention: SIEM systems generate massive amounts of data, and retaining this data for compliance and investigative purposes can be challenging due to storage costs and regulatory requirements.

SOAR technology complements SIEM by automating incident response processes, orchestrating security tools, and providing a centralized platform for managing security operations. SOAR solutions offer several benefits to the oil and gas industry, including:

- Improved Efficiency of Security Operations: SOAR solutions streamline security operations by automating repetitive tasks, such as threat intelligence gathering, vulnerability assessment, and incident response.

- Threat Detection and Intelligence: SOAR solutions enhance threat detection by integrating with various security tools and threat intelligence feeds, providing a more comprehensive view of the threat landscape. This allows oil and gas companies to stay ahead of emerging threats and proactively defend against potential attacks.

- Accelerated Incident Response Process: SOAR solutions accelerate incident response by automating tasks such as malware analysis, containment, and eradication, enabling faster resolution of security incidents. SOAR solutions can help oil and gas companies improve their incident response time by automating tasks such as malware analysis and containment, minimizing the impact of security incidents.

- Reduced MTTD and MTTR: SOAR solutions help reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents by automating and orchestrating incident response processes.

- Faster Incident Response: SOAR solutions can speed up incident response by enabling teams to view all relevant data tied to potential breaches as they occur. This centralized view of security data allows for faster and more effective decision-making during incident response.

- Productivity Boost of Security Teams: SOAR solutions free up security teams from mundane tasks, allowing them to focus on more strategic initiatives, such as threat hunting and vulnerability management.

- Addressing Alert Fatigue: SOAR solutions help mitigate alert fatigue by automating the analysis and triage of security alerts, allowing security teams to focus on the most critical threats.

- Vendor-Agnostic Integration: A key benefit of SOAR is its ability to integrate with a wide range of security tools and technologies. This is particularly important for oil and gas companies that often have diverse security infrastructure, allowing them to seamlessly integrate SOAR with their existing systems.

- Automation and Human Expertise: While SOAR solutions automate many security tasks, they are not intended to replace security professionals. SOAR complements human expertise by automating repetitive tasks and providing analysts with the information they need to make informed decisions.

Despite these benefits, SOAR solutions also have limitations, such as:

- Integration Complexity: Integrating SOAR solutions with existing security tools and infrastructure can be complex and require significant effort, potentially delaying the realization of SOAR benefits.

- Planning and Design: The success of SOAR implementation depends on careful planning and design, including identifying appropriate use cases, defining workflows, and integrating with existing security tools.

- Maintenance and Updates: SOAR solutions require ongoing maintenance and updates to ensure they remain effective and compatible with evolving security threats and technologies. The lack of skilled personnel to manage and operate SOAR solutions can limit their effectiveness in automating security operations.

- Legacy System Integration: The integration of SOAR solutions with legacy systems can be challenging, potentially hindering the automation of incident response processes.

V. BEST PRACTICES FOR SIEM AND SOAR IMPLEMENTATION IN OIL AND GAS

To ensure successful SIEM implementation in the oil and gas industry, organizations should clearly define specific and measurable goals, such as improving threat detection rates, reducing incident response times, and meeting compliance requirements. They must prioritize critical data sources by focusing on systems and applications that handle sensitive information or are crucial for operational continuity. Implementing correlation rules aligned with security objectives and industry best practices is essential, as is configuring automated alerts for critical security events to ensure timely responses. Regularly reviewing logs from endpoints, servers, and network devices helps identify potential threats and anomalies. Compliance with relevant regulations, such as the NIST Cybersecurity Framework, should be ensured, while staff should receive regular training on SIEM tools, best practices, and incident response procedures. Clear incident response protocols must be established, and the performance of the SIEM system should be continuously monitored to address bottlenecks or performance issues. Keeping the SIEM system updated with the latest patches and threat intelligence is vital, as is starting with a smaller implementation and scaling gradually as expertise develops. Comprehensive logging should capture data from all relevant sources, including firewalls, servers, applications, and intrusion detection systems. SIEM rules and policies must be periodically reviewed and updated to address evolving threats. Ongoing training on new SIEM features, best

practices, and threat intelligence is necessary for the security team. Measures to ensure data integrity, such as encryption, access controls, and regular backups, should be implemented, alongside strategies to address data retention challenges through efficient classification, compression, and tiered storage. Balancing data retention with system performance requires optimized storage solutions, indexing, and data summarization techniques. Aligning with compliance requirements involves working closely with legal and compliance teams to create flexible retention policies. Finally, organizations must consider industry-specific needs, such as protecting operational technology (OT) systems and ensuring the security of critical infrastructure, to address the unique cybersecurity challenges of the oil and gas sector.

To maximize the benefits of SOAR in the oil and gas industry, organizations should clearly define the security focus, such as improving incident response times, enhancing threat detection, or automating specific security tasks. Setting realistic goals based on the organization's resources, security maturity, and risk appetite is crucial for effective implementation. SOAR should foster collaboration between security teams, IT operations, and other stakeholders, while prioritizing ease of use by selecting a solution that integrates seamlessly with existing security tools. Developing clear and concise playbooks for various security scenarios ensures consistent incident response and automation. Regular training and simulation exercises help equip the security team to handle real-world incidents effectively. Before implementation, organizations should assess their capabilities, needs, and commitment to SOAR, considering the scope and scale of customers, business operations, and platforms. Applying data standards and ensuring regular data cleaning and normalization optimizes SOAR performance. An organized approach to playbooks and workflows promotes efficiency, while continuous monitoring identifies areas for improvement. Addressing industry-specific challenges, such as protecting OT networks and critical infrastructure, is essential for the oil and gas sector. Organizations must also tackle challenges like a lack of skilled staff through hiring and training initiatives and leverage SOAR to enhance automation and orchestration in security operations. Recognizing that SOAR is an evolving technology, organizations should adapt their strategies to address new threats and security challenges as they arise.

VI. CONCLUSION

SIEM and SOAR are essential tools for oil and gas companies that want to improve their cybersecurity posture and protect their critical infrastructure and sensitive data. By implementing these technologies and following best practices, oil and gas companies can enhance their ability to detect, respond to, and mitigate cyber threats in real-time.

When considering implementing SIEM and SOAR, oil and gas companies should:

- Conduct a thorough risk assessment: Identify the organization's most critical assets and the potential threats they face.
- Define clear security objectives: Determine the specific goals that the organization wants to achieve with SIEM and SOAR.
- Select solutions that align with their specific needs and budget: Evaluate different SIEM and SOAR solutions and choose those that best meet the organization's requirements.
- Develop a comprehensive implementation plan: This plan should include data source integration, security workflow automation, and staff training.

- Establish a process for ongoing monitoring and evaluation: Regularly monitor and evaluate the performance of the SIEM and SOAR solutions to ensure they are meeting the organization's security objectives.

By taking these steps, oil and gas companies can effectively leverage SIEM and SOAR to improve their cybersecurity posture and protect their operations from the ever-evolving threat landscape.

VII. REFERENCES

[1] Larsen, Gregory, et al. "State-of-the-art resources (soar) for software vulnerability detection, test, and evaluation." Institute for Defence Analysis, Virginia, USA, Tech. Rep. IDA Paper P-5061 (2014).
[2] Kavanagh, Kelly M., Oliver Rochford, and Toby Bussa. "Magic quadrant for security information and event management." Gartner Group Research Note (2015).
[3] Fannin, Richard S. Bridging the gap between the utility industry and the customer. MS thesis. The College of St. Scholastica, 2017.
[4] Ramos, Sofia B., and Helena Veiga. "Risk factors in oil and gas industry returns: International evidence." Energy Economics 33.3 (2011): 525-542.
[5] Coppolino, Luigi, et al. "Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study." Computer Safety, Reliability, and Security: 30th International Conference, SAFECOMP 2011, Naples, Italy, September 19-22, 2011. Proceedings 30. Springer Berlin Heidelberg, 2011.
[6] Lamba, Anil. "Protecting 'cybersecurity &resiliency'of nation's critical infrastructure–energy, oil & gas." International Journal of Current Research 10 (2018): 76865-76876.
[7] Briesemeister, Linda, et al. "Detection, correlation, and visualization of attacks against critical infrastructure systems." 2010 Eighth International Conference on Privacy, Security and Trust. IEEE, 2010.
[8] Hindy, Hanan, et al. "Improving SIEM for critical SCADA water infrastructures using machine learning." International Workshop on Security and Privacy Requirements Engineering. Cham: Springer International Publishing, 2018.
[9] Singh, Vivek Kumar, Steven Perez Callupe, and ManimaranGovindarasu. "Testbed-based evaluation of siem tool for cyber kill chain model in power grid scada system." 2019 North American Power Symposium (NAPS). IEEE, 2019.
[10] Gao, Yuan, et al. "SIEM: policy-based monitoring of SCADA systems." (2016).
[11] Nazir, Sajid, Shushma Patel, and Dilip Patel. "Assessing and augmenting SCADA cyber security: A survey of techniques." Computers & Security 70 (2017): 436-454.
[12] Hadbah, Abdulrahman, Akhtar Kalam, and Hassan Al-Khalidi. "The subsequent security problems attributable to increasing interconnectivity of SCADA systems." 2008 Australasian Universities Power Engineering Conference. IEEE, 2008.
[13] Morsey, Christopher. Supervisory Control and Data Acquisition (SCADA) Systems and Cyber-Security: Best Practices to Secure Critical Infrastructure. Robert Morris University, 2017.
[14] Singh, Vivek Kumar, Steven Perez Callupe, and ManimaranGovindarasu. "Testbed-based evaluation of siem tool for cyber kill chain model in power grid scada system." 2019 North American Power Symposium (NAPS). IEEE, 2019.