OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.19915635

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue-02|2026

Enhancing Protection Against Social Engineering Attacks in the Nigerian Financial Sector Using SOAR-Driven Automated Incident Response

Nonye Peter Awurum

Charisma University, USA and British Training Center, UAE

Article History
Received: 20.03.2026
Accepted: 25.04.2026
Published: 30.04.2026

Citation
Awurum, N. P. (2026). Enhancing Protection Against Social Engineering Attacks in the Nigerian Financial Sector Using SOAR-Driven Automated Incident Response. *Indiana Journal of Multidisciplinary Research, 6*(2), 9-23.

Abstract: Social engineering attacks continue to pose a significant and evolving threat to the Nigerian financial sector, where rapid digitalization, high transaction volumes, and widespread reliance on electronic banking channels increase exposure to human-focused cyberattacks. Phishing, business email compromise, credential harvesting, and social-media-enabled impersonation remain major attack vectors that routinely bypass traditional security controls by exploiting human vulnerabilities. To address this challenge, this study investigates the application of Security Orchestration, Automation, and Response (SOAR) platforms as a technical and procedural mechanism for reducing susceptibility to social engineering attacks and minimizing the impact of successful breaches. The research develops realistic social engineering scenarios reflecting common Nigerian threat patterns—including brute-force credential attacks, unauthorized account access, data exfiltration, and malware-enabled compromise—and maps them to automated SOAR playbooks triggered by SIEM-generated alerts. These playbooks perform actions such as automated account lockdowns, forced password resets, anomaly-based detection of suspicious login activity, and user-targeted security notifications. Findings demonstrate that SOAR-driven responses significantly reduce response time, enhance containment of post-breach activity, and improve overall cyber resilience within financial institutions. The study further highlights the relevance of SOAR in alleviating the strain on Nigerian cybersecurity teams facing persistent skill shortages. Importantly, the integration of automated incident response supports strengthened compliance with sectoral regulatory expectations, particularly those issued by the Central Bank of Nigeria (CBN) and the Nigeria Data Protection Commission (NDPC), by enhancing auditability, incident tracking, and timely remediation. While SOAR cannot fully prevent social engineering, it serves as a critical complementary measure within a multilayered cybersecurity architecture across Nigeria's financial ecosystem.

Keywords: Cybersecurity Oversight, Board of Directors (BoD), Institutional Theory, Director Engagement, Corporate Governance, Cyber-expertise, Coercive Pressures,Risk Management,

INTRODUCTION

There's no doubt that cybersecurity is a priority for enterprises today. While the exact future of remote work is still somewhat up in the air, the recent shifts in employee arrangements have opened the door to new (and often unanticipated) threats.

Between 2019 and mid-2020, 16 billion records were exposed, including everything from credit card numbers to medical information.

Social engineering (SE) has become a dominant threat vector in contemporary cybersecurity, shifting adversarial focus from purely technical exploitation toward the manipulation of human behavior. Social engineering attacks intentionally target individuals—rather than systems—using deception and psychological techniques to elicit actions such as credential disclosure, malicious link execution, or policy violations that can enable unauthorized access to organizational resources (Krombholz *et al.*, 2015; Washo, 2021). In practice, SE undermines the "human firewall," leveraging social and cognitive factors to bypass technical defenses that are otherwise effective against conventional malware-centric attacks (Mouton *et al.*, 2015; Mitnick & Simon, 2006). Industry and scholarly accounts frequently associate a substantial proportion of security incidents with human error, reinforcing the view that human-centric attacks are both prevalent and consequential in organizational environments (Evans *et al.*, 2016; Coffey, 2017).

The financial sector is particularly vulnerable to social engineering due to the high value of financial and customer data, the operational dependency on digital channels, and the severe business consequences of breaches, including financial losses and reputational damage (Edwards *et al.*, 2017; Krombholz *et al.*, 2015). A further challenge is that early phases of well-executed SE attacks may contain no obvious malicious payload, making them difficult to detect through traditional technical controls at the initial stage (Krombholz *et al.*, 2015; ENISA, 2022). As a result, risk reduction often depends not only on prevention but also on timely detection, containment, and recovery once anomalous behavior becomes observable in logs and telemetry (Chiconski *et al.*, 2012; Ross *et al.*, 2021).

***Corresponding Author:** Nonye Peter Awurum

Organizations commonly rely on security awareness training to mitigate SE risk, with effectiveness often assessed using internal phishing simulations and user click rates (Pratt, 2021; Evans *et al.*, 2016). However, training alone is widely viewed as insufficient because human behavior is context-dependent and may be influenced by relationships, perceived consequences, and situational pressures; accordingly, awareness interventions may reduce but rarely eliminate SE susceptibility (Alruwaili, 2019; Evans *et al.*, 2016). This limitation is exacerbated by the persistent shortage of skilled cybersecurity professionals, which constrains the ability of organizations to sustain rapid, consistent, analyst-driven incident response at scale (Naseer *et al.*, 2021; Kinyua & Awuah, 2021).

In response, Security Orchestration, Automation, and Response (SOAR) platforms have emerged as a practical capability for improving the efficiency and consistency of security operations by automating investigation and incident response workflows through configurable playbooks (Bridges *et al.*, 2022; Kinyua & Awuah, 2021). SOAR complements Security Information and Event Management (SIEM) systems by enabling orchestration across tools and executing response actions automatically after detection rules trigger incidents (Bridges *et al.*, 2022; Sridharan & Kanchana, 2022). Importantly, SOAR is not intended to replace human analysts but to amplify their impact by reducing repetitive workload and accelerating standardized response actions, a capability increasingly relevant in resource-constrained environments (Kinyua & Awuah, 2021; Islam *et al.*, 2020).

Because social engineering frequently culminates in observable post-compromise indicators (e.g., anomalous logins, data transfer anomalies, endpoint detections), SOAR is particularly well-suited to reducing the consequences of successful SE by enabling rapid containment and remediation (Odeh *et al.*, 2021; Kinyua & Awuah, 2021). Nevertheless, the literature also emphasizes that no single control is a "silver bullet" against social engineering; effective risk reduction requires layered socio-technical measures integrating awareness, detection, response processes, and supportive technologies (Washo, 2021; Petrescu, 2023). Accordingly, this study situates SOAR-driven automated incident response as a complementary mechanism within a broader security architecture, examining how automation can reduce exposure to SE-related incidents by shortening response time, improving containment, and strengthening operational resilience in regulated financial environments (Chiconski *et al.*, 2012; Kinyua & Awuah, 2021).

Some of the top SOAR Platforms in 2026 are

- Splunk SOAR
- Palo Alto Networks Cortex XSOAR
- Fortinet FortiSOAR
- Swimlane
- Microsoft Sentinel

TECHNICAL CONCEPTS

Social Engineering

Social engineering refers to a category of cyberattacks in which adversaries exploit human trust, psychology, and social dynamics in order to manipulate individuals into performing actions that compromise information systems (Chetioui *et al.*, 2021; Hatfield, 2018). Unlike attacks that target software vulnerabilities, social engineering bypasses technological controls by persuading victims—through deception, impersonation, or psychological pressure—to disclose sensitive information or unintentionally facilitate unauthorized access (Mouton *et al.*, 2015; Washo, 2021). Within financial institutions, where employees frequently engage with customers, high-value transactions, and sensitive records, attackers leverage techniques such as phishing, spear-phishing, pretexting, and business email compromise (BEC) to gain initial footholds into corporate networks (ENISA, 2022; Edwards *et al.*, 2017).

The effectiveness of social engineering arises from its manipulation of psychological triggers—authority, time pressure, scarcity, reciprocation, commitment, social proof, and friendship—which influence decision-making and increase the likelihood of human error (Butavicius *et al.*, 2015; Mouton *et al.*, 2016). As prior research highlights, human error plays a role in the majority of cyber incidents, making social engineering a persistent and highly effective attack vector against both individuals and organizations (Evans *et al.*, 2016; Coffey, 2017).

Cyber Incident Response

Cyber incident response encompasses the structured processes and activities required to detect, analyze, contain, eradicate, and recover from cybersecurity incidents (Naseer *et al.*, 2021; van der Kleij *et al.*, 2022). According to the National Institute of Standards and Technology (NIST), a cyber incident involves actions that compromise the confidentiality, integrity, or availability of information systems (NIST; NCSC, 2016). Financial institutions are particularly sensitive to disruptions due to regulatory requirements, operational risks, and the criticality of continuous service delivery.

The NIST Incident Response Life Cycle (Cichonski *et al.*, 2012) comprises four phases:

1. **Preparation** – establishing policies, tools, skills, and procedures to respond effectively.
2. **Detection and Analysis** – identifying anomalous activities and validating whether they constitute security incidents.
3. **Containment, Eradication, and Recovery** – limiting damage, removing adversary artifacts, and restoring normal operations.

***Corresponding Author:** Nonye Peter Awurum

4. **Post-Incident Activity** – extracting lessons learned and improving response capabilities.

Incident response within financial institutions must remain agile, auditable, and capable of addressing both technical and human-centered attacks. Social engineering incidents often require rapid detection and containment because attackers may exploit compromised credentials, initiate unauthorized transactions, or exfiltrate sensitive customer data. The increasing complexity and frequency of incidents underscore the importance of structured processes supported by automation and coordinated security tooling.

Security Orchestration, Automation, and Response (SOAR)

SOAR refers to a variety of technologies that help organizations collect data from across the network, including from their security operations team (SOC team). These tools are there to help people define and drive a logical incident response — one that is standardized across departments.

The three components of SOAR work together to optimize organizational security objectives.

Security orchestration integrates multiple security tools into one framework. When automated detection is insufficient, technical staff (e.g., security analysts, architects, administrators) provide support. This component helps organizations enhance incident response by automating repetitive, low-level tasks and allowing cybersecurity teams to focus on higher-value work.

Automation uses machines to handle routine security tasks. SOAR tools streamline investigations and accelerate response by combining automated actions with human decision-making.

Cybersecurity teams define procedures for the below steps; and these steps form the security automation playbook.

- Automated actions
- Decision-making
- Monitoring and auditing
- Enforcement tasks

Response enables cybersecurity teams to act on incidents, collaborate effectively, and maintain shared knowledge for resolving threats. Key response functions include:

- Alert Prioritization and Processing: SOAR collects data from security systems. Analysts validate threats, assess related risks, and trigger coordinated response activities with the Security Operations Center.
- Threat Intelligence Management: SOAR gathers vulnerability data, which analysts convert into actionable intelligence for proactive defense.
- Dashboard and Reporting: SOAR generates reports and dashboards for all security stakeholders—SOC managers, CISOs, analysts—helping them understand threats and improve cybersecurity measures.

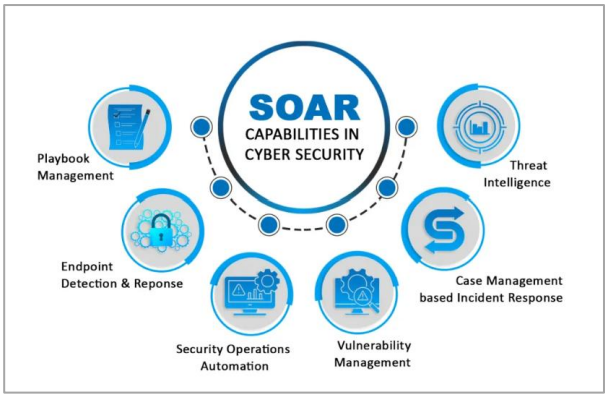

Figure 1: SOAR Capabilities in Cybersecurity

Note. The figure 1 below illustrates the core capabilities of Security Orchestration, Automation, and Response (SOAR) in cybersecurity operations. Key components include playbook management, threat intelligence, case-based incident response, vulnerability management, security operations automation, and endpoint detection and response.

These elements collectively demonstrate how SOAR enhances efficiency, coordination, and speed in responding to cyber threats.

It is observed that the SOAR (Security Orchestration, Automation, and Response) technology acts as the central nerve center of a modern Security Operations Center (SOC), integrating disparate security tools to automate incident response and reduce manual labor. While SIEM (Security Information and Event Management) focuses on data collection, logging, and detecting threats, SOAR picks up where SIEM stops by providing the action-oriented tools to respond to those threats. SIEM acting as the "eyes" and SOAR acting as the "hands" of the security operation

SOAR platforms are emerging technologies designed to automate, coordinate, and streamline security operations tasks, particularly those performed within security operations centers (Bridges *et al.*, 2022). SOAR integrates with SIEM systems to ingest alerts, enrich context, correlate events, and execute automated playbooks that standardize incident response workflows (Mohsienuddin Mohammad & Lakshmisri, 2018). While SIEM platforms focus on log aggregation and detection, SOAR extends these capabilities by enabling automated mitigation actions such as credential resets, account lockdowns, device isolation, and alert triage (Sridharan & Kanchana, 2022).

***Corresponding Author:** Nonye Peter Awurum

Automation is particularly useful where cyber skills shortages make manual incident handling difficult to sustain at scale (Kinyua & Awuah, 2021). SOAR does not replace human analysts; rather, it enhances security teams' efficiency by automating repetitive tasks and accelerating response processes. Given that social engineering attacks often produce detectable events—such as unusual login patterns, suspicious file transfers, or endpoint malware prevention—SOAR provides a mechanism to reduce the consequences of human error by enabling rapid, consistent, and policy-driven containment actions (Odeh *et al.*, 2021; Kinyua & Awuah, 2021).

MITRE ATT&CK Framework

The MITRE ATT&CK framework serves as a comprehensive, globally recognized knowledge base for describing adversarial tactics, techniques, and procedures (Blake *et al.*, 2020). Designed to provide a common taxonomy for analyzing and classifying cyberattacks, ATT&CK supports both researchers and security teams in identifying behavioral patterns and mapping detection or mitigation strategies to known adversarial actions (Georgiadou *et al.*, 2021).

For enterprise environments, including financial institutions, MITRE ATT&CK helps structure threat analysis by categorizing activities such as credential access, lateral movement, privilege escalation, and data exfiltration. By mapping SOAR detections and automated responses to ATT&CK techniques, organizations can ensure standardized classification, improve threat modeling, and support more effective incident response (Tatam *et al.*, 2021; Irshad & Basit Siddiqui, 2022).

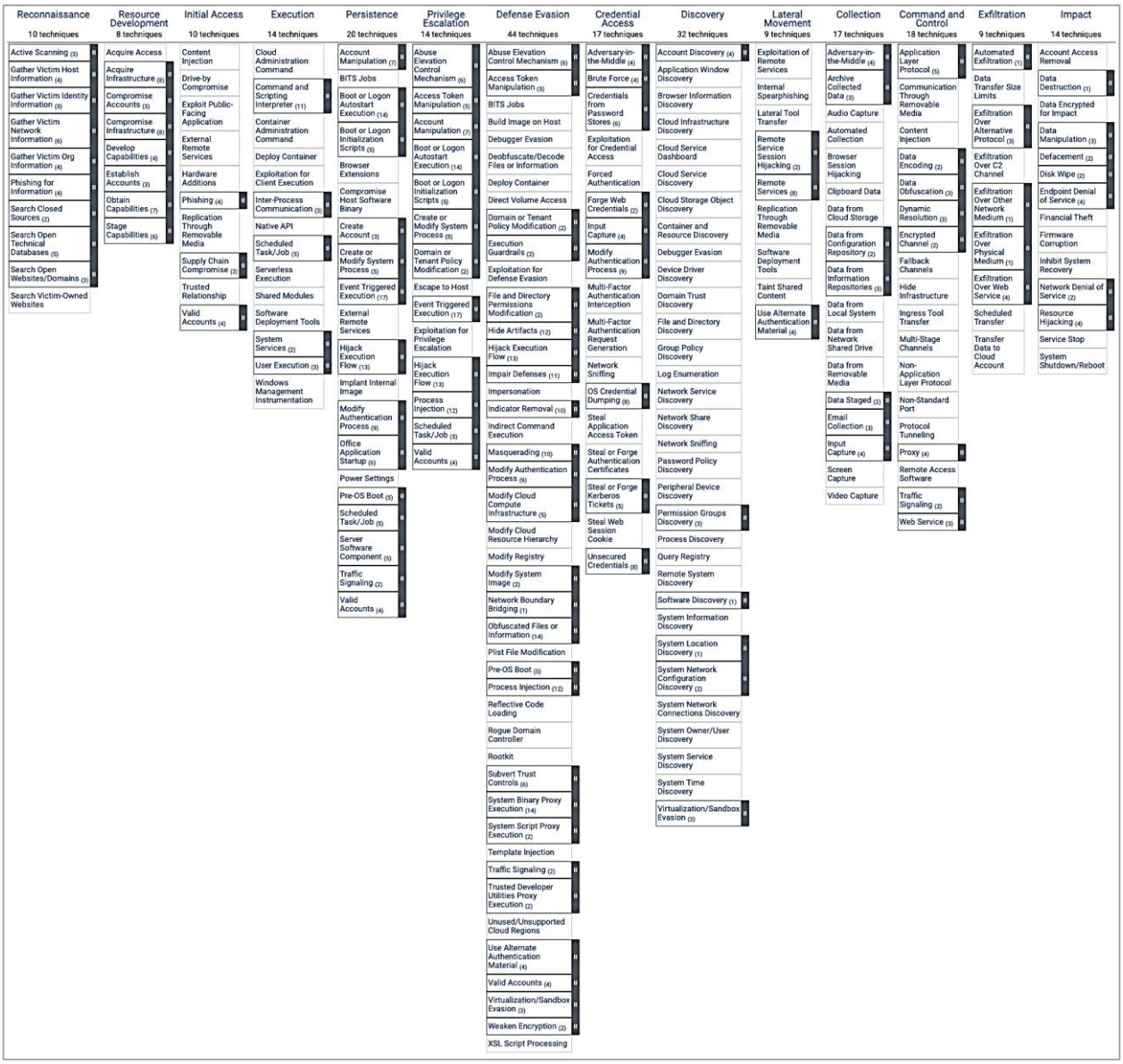

Figure 2: MITRE ATT&CK Framework.

Note: Figure 2 below is the MITRE ATT&CK® framework, which is a comprehensive, globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world, observed cyberattacks. It functions as a behavioral model for security teams to map, detect, and analyze attacker behavior across the entire lifecycle, rather than just focusing on malware signatures.

MATERIALS AND METHODS

This study adopts a design-science research orientation to develop, demonstrate, and evaluate SOAR-enabled measures aimed at reducing the impact of social engineering attacks within the Nigerian financial sector. The approach aligns with the objectives of design science, which emphasize the creation of practical, context-relevant artifacts that address organizational problems through iterative development and evaluation (Peffers *et al.*, 2007). The methodology integrates qualitative research, vignette construction, and technical artifact development to reflect realistic threat conditions experienced by financial institutions.

Design Science Research Methodology (DSRM)

Design Science Research Methodology (DSRM) provides a structured framework for addressing problem-oriented and application-oriented research questions through the creation of innovative artifacts (Venable *et al.*, 2017; Peffers *et al.*, 2007).

Table 3.1 below summarizes how Design Science Research Methodology (DSRM) stages are operationalized in the study, linking each phase to concrete outputs such as vignette development, SOAR playbooks, and evaluation evidence.

Table 3.1: Design Science Research Methodology (DSRM) Mapping for the Study

DSRM Stage	Purpose in This Study	Key Outputs/Artifacts
Problem Identification & Motivation	Establish the persistent risk of social engineering in financial institutions and the need for automation to reduce post-compromise impact.	Problem statement; scope; context assumptions
Define Objectives of a Solution	Specify what "improved protection" means operationally (speed, containment, consistency, auditability).	Design objectives; success criteria
Design & Development	Build SOAR artifacts (playbooks) and detection logic using SIEM telemetry and automation workflows.	Playbooks; analytic rules; automation rules; ATT&CK mappings
Demonstration	Execute vignettes (simulated scenarios) to show that detection triggers and playbooks run as intended.	Demonstration logs; execution evidence
Evaluation	Assess whether the artifacts reduce exposure through automated containment and user feedback.	Evaluation results; performance assessment
Communication	Present findings and implementation guidance for financial institutions.	Reported outcomes; implementation recommendations

In this study, the identified problem is the persistent vulnerability of financial-sector employees to social engineering attacks, particularly those involving credential harvesting, unauthorized access, and post-compromise exploitation. The candidate solution—SOAR-enabled automated incident response—requires empirical assessment, making DSRM an appropriate methodological foundation.

The research process follows Peffers *et al.*'s (2007) stages, beginning with problem identification, deriving objectives for a technological solution, designing and developing SOAR playbooks, demonstrating their functionality using representative scenarios, and evaluating their effectiveness. The development of artifacts occurs using Microsoft Sentinel, selected for its mature SOAR capabilities and compatibility with common security architectures deployed across financial institutions.

The figure depicts the end-to-end study workflow: problem framing, solution objectives, expert-informed vignette design, SOAR artifact development, demonstration through scenario execution, and evaluation of incident response outcomes.

***Corresponding Author:** Nonye Peter Awurum

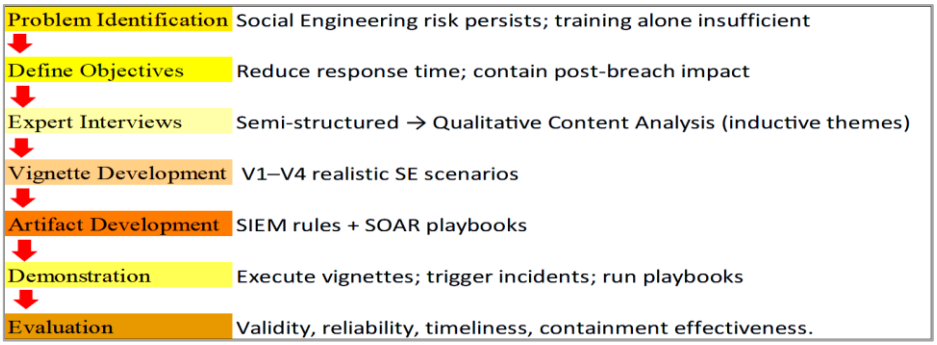

Figure 3.1: Study Method Flow (DSRM + Qualitative Inputs + Artifact Demonstration)

Qualitative Research Using Expert Interviews

Given the complexity of social engineering attacks and the emerging nature of SOAR platforms in operational settings, qualitative data collection was conducted through semi-structured interviews with cybersecurity practitioners. Semi-structured interviews allow flexibility to explore domain-specific knowledge, contextual challenges, and practical constraints that influence security operations (Mayring, 2022).

In Table 3.2 below, the interview strategy and qualitative content analysis approach are presented to clarify data sources, handling procedures, and the inductive derivation of themes used to guide vignette creation and SOAR playbook design.

Table 3.2: Expert Interview Strategy and Data Handling

Component	Description
Interview Type	Semi-structured interviews to capture practitioner perspectives on SE threats, incident response gaps, and SOAR feasibility.
Sampling Approach	Purposive selection for diversity across security operations, IAM, incident response, and governance roles to reduce shared bias.
Data Capture	Interviews recorded and transcribed for systematic analysis.
Analysis Method	Qualitative content analysis with inductive category formation to minimize preconceptions and derive themes from data.
Use of AI Tools	If used at all, AI output treated as supplementary due to hallucination risk; human expert insights prioritized.
Outputs	Categories/themes informing vignette selection and playbook design (e.g., compromised accounts, exfiltration, awareness feedback).

Consistent with the source study's methodological choices, expert participants were selected based on their experience in cybersecurity subdomains such as incident response, automation, identity and access management, threat detection, and security governance. The recruitment strategy emphasized variation in job roles, experience levels, and industry contexts to mitigate shared-bias risks and ensure a diverse set of insights (Waelchli & Walter, 2025). Interviews were recorded, transcribed, and subjected to qualitative content analysis to identify recurring themes related to social engineering risks, incident response gaps, and opportunities for SOAR integration.

As in the original study, inductive category formation was used to minimize the bias introduced by preconceived assumptions (Mayring, 2022). Interview outputs directly informed the design of social engineering vignettes and guided the selection of automation tasks within SOAR playbooks. Although large language models may produce unreliable information, the source methodology incorporated one AI-based interview with appropriate safeguards; however, in the present study such data were used only supplementary to human expert perspectives.

Social Engineering Vignettes and Use-Case Development

To model realistic risks within the Nigerian financial sector, the study developed four social engineering vignettes mirroring common attacker behaviors:

- **Brute-force attacks on user accounts**, often following credential exposure or OSINT-enabled profiling.
- **Data exfiltration** after device compromise or unauthorized access.
- **Compromised user accounts** resulting from phishing or absent multi-factor authentication.
- **Malware-enabled compromise**, where adversaries capitalize on user error to deploy malicious payloads.

Table 3.3 below shows where the Vignettes represent realistic social engineering–related scenarios and corresponding observable signals typically captured in security telemetry; they function as controlled test cases for demonstrating and evaluating SOAR-enabled automated incident response.

***Corresponding Author:** Nonye Peter Awurum

Table 3.3: Social Engineering Vignettes Used for Demonstration

Vignette ID	Scenario (Social Engineering–Related)	Observable Signals (Telemetry)	Intended Risk Reduced
V1	Brute-force attempt against a user account following OSINT-derived username/email.	Excessive failed login attempts; credential access indicators	Prevent credential compromise; reduce account takeover exposure
V2	Data exfiltration to an unapproved cloud storage service after user/device compromise.	High-volume uploads to external cloud service; unusual file transfer patterns	Reduce data loss and dwell time
V3	Compromised credentials used for suspicious login (e.g., atypical location/behavior) to access enterprise resources.	Anomalous sign-ins; atypical access to cloud resources	Contain compromised account rapidly
V4	User executes malicious link/attachment; endpoint protection blocks malware; user may be unaware.	EDR prevention events; malware blocked alerts	Reinforce awareness through real-incident notification

These vignettes serve as controlled scenarios for testing SOAR automation. They allow evaluation of detection logic, response timing, and the operational robustness of integrated playbooks. Each vignette was designed such that the triggering events correspond to signals typically captured in SIEM platforms (e.g., anomalous login patterns, unauthorized file transfers, endpoint alerts), ensuring alignment with realistic telemetry generated by financial institutions.

Artifact Development and SOAR Playbook Construction

Following insights from expert interviews and vignette design, SOAR artifacts were developed in Microsoft Sentinel using Logic Apps. These artifacts include automated workflows to:

- **Lock user accounts** after detection of suspicious activity
- **Enforce password resets** to disrupt adversarial persistence
- **Notify users** of blocked malware or prevented attacks
- **Coordinate multiple detection and automation rules** mapped to MITRE ATT&CK classifications

The playbooks in Table 3.4 summarize automated incident response actions triggered by SIEM incidents, including account containment and user notification measures designed to reduce exposure following suspected social engineering compromise

Table 3.4: SOAR Playbooks and Automated Response Actions

Playbook	Trigger Condition (SIEM Incident)	Automated Actions	Security Objective
PB1: Force Password Reset	Brute-force detection or suspicious credential activity incident.	Enforce password change; optional notification	Disrupt credential abuse; reduce persistence
PB2: Block/Lock User Account	Data exfiltration incident or compromised account signal.	Disable/lock account; optional notification	Rapid containment and account takeover prevention
PB3: User Notification of Prevented Malware	EDR detects and blocks malware execution initiated by user action.	Notify affected user; awareness reinforcement	Strengthen human behavior via immediate feedback

In figure 3.2, the mapping links each vignette to its corresponding SOAR playbook, illustrating how specific attack signals initiate predefined response actions such as password resets, account lockdowns, or user notifications.

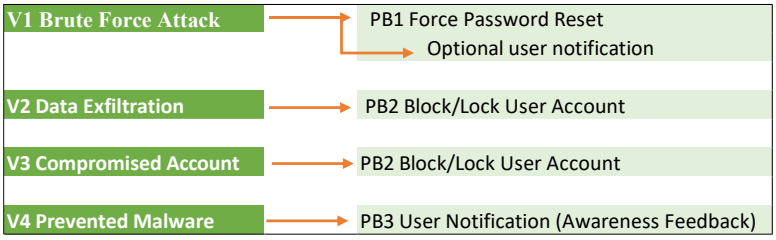

Figure 3.2: Mapping of Vignettes to SOAR Playbooks

***Corresponding Author:** Nonye Peter Awurum

Each playbook integrates with Sentinel's analytic and automation rules to ensure that incidents generated by the SIEM automatically trigger the appropriate containment actions. The design emphasizes rapid response, reduction of human workload, and agility in handling SE-related incidents that may progress quickly.

In figure 3.3, the control loop model conceptualizes how telemetry feeds SIEM detection, which triggers SOAR orchestration and automated response actions, producing measurable containment outcomes and enabling continuous improvement through tuning and expansion of vignettes and playbooks.

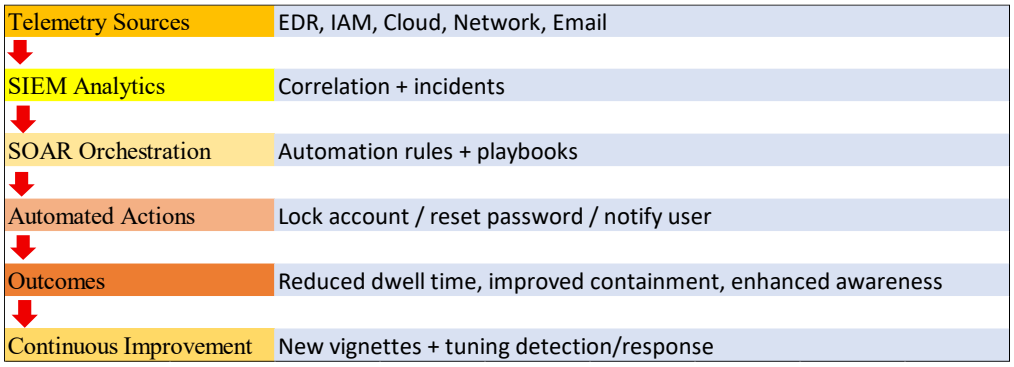

Figure 3.3: SOAR Enabled Response Logic (Conceptual Control Loop)

Demonstration and Evaluation

The artifacts were demonstrated by executing each vignette to validate detection rules fired correctly and that associated playbooks executed the intended response actions. For example, brute-force login attempts were simulated to test credential-access detections, data exfiltration was modeled through unauthorized cloud uploads, and anomalous login patterns were generated via geolocation anomalies.
Evaluation criteria included:

- accuracy of incident detection,
- speed and reliability of automated response execution,
- effectiveness of containment actions, and
- operational feasibility within a financial-sector security architecture.

Consistent with the findings in the source study, SOAR measures effectively reduced exposure by automating post-compromise actions that would otherwise rely on manual intervention.

Evaluation criteria define how artifact performance is assessed during demonstration, including detection validity, automation reliability, timeliness, containment effectiveness, and practical feasibility within operational constraints.

Table 3.5: Evaluation Criteria for Demonstration and Artifact Effectiveness

Evaluation Dimension	Operational Definition	Evidence Collected
Detection Validity	Whether analytic rules generate the correct incident for each vignette scenario.	Incident logs; SIEM alerts
Automation Reliability	Whether playbooks execute consistently once incidents are created.	Playbook run history; workflow outputs
Response Timeliness	Time from incident generation to containment action completion.	Time stamps from SIEM and SOAR
Containment Effectiveness	Whether response actions (lock/reset/notify) reduce post-compromise exposure.	Account state changes; prevention records
Human-Centered Impact	Whether notifications and enforced actions reduce user vulnerability post-event.	Notification evidence; awareness feedback rationale
Practical Feasibility	Fit within operational constraints and SOC capacity (skills shortage motivation).	Implementation notes; workload rationale

Section 4 presents the demonstration outcomes and evaluation results of the SOAR playbooks across the defined social engineering vignettes.

RESULTS

This section reports the outcomes of the qualitative inquiry and the demonstration/evaluation of SOAR-driven automated incident response for social engineering–related scenarios. The results are presented in three parts: (i) themes derived from expert inputs and their implications for SOAR adoption, (ii) the operationalization of vignettes into SIEM detections and SOAR playbooks, and (iii) demonstration outcomes and evaluation against predefined criteria. The end-to-end workflow guiding these results is summarized in **Figure 3.1**.

***Corresponding Author:** Nonye Peter Awurum

4.1 Practitioner Perspectives on Social Engineering, Skills Constraints, and SOAR Utility

Analysis of expert perspectives (captured and synthesized via the qualitative process described in **Table 3.2**) indicates broad agreement that contemporary cyber threats increasingly exploit human vulnerabilities and that social engineering remains among the most acute and persistent risks. In particular, practitioners emphasized that (a) awareness training positively influences employee behavior but cannot eliminate risk, (b) successful social engineering incidents frequently lead to high-impact consequences (e.g., unauthorized access and data exposure), and (c) cybersecurity skills shortages constrain the ability of security teams to respond rapidly and consistently at scale. These findings reinforce the need for complementary, technology-enabled controls beyond training, including automated incident response mechanisms.

Participants further noted that SOAR capabilities are most valuable in **post-breach** or **post-compromise** phases—when suspicious behaviors become observable in telemetry—by triggering standardized containment actions such as account lockouts or credential resets. This perspective aligns with the study's design objective to reduce the consequences of human error by shortening response time and automating repeatable containment steps (see **Table 3.1** and **Figure 3.3**).

Social Engineering Vignettes and Corresponding SOAR Measures

Guided by the qualitative insights and the objective to create actionable SOAR artifacts (see **Table 3.1**), four social engineering vignettes were developed to represent realistic threat patterns that can occur in financial environments (see **Table 3.3**). These vignettes focus on (V1) brute-force credential attacks, (V2) data exfiltration via unauthorized cloud services, (V3) compromised account usage with anomalous login behavior, and (V4) awareness enhancement through user notification after malware prevention events.

Each vignette was operationalized using SIEM analytic rules and automation rules to generate incidents and trigger SOAR playbooks (see **Table 3.4**). As shown in **Figure 3.2**, vignettes V2 and V3 map to account blocking/lockout actions, V1 maps to a forced password reset response, and V4 maps to user notification to provide immediate feedback and reinforce awareness following a real prevented attack.

Consistent with structured threat classification practice, detections were mapped to relevant MITRE ATT&CK tactics/techniques to support standardization and future tuning. The resulting artifact suite constitutes a set of automated safeguards designed to reduce exposure after the initial social engineering stage by containing suspicious activity once detectable signals are produced in logs and endpoint telemetry (see **Figure 3.3**).

Demonstration Outcomes and Evaluation

Demonstration was conducted by executing each vignette scenario and observing whether (i) detection logic generated an incident and (ii) the appropriate SOAR playbook executed the intended containment/notification actions. The evaluation followed the criteria defined in **Table 3.5** (detection validity, automation reliability, response timeliness, containment effectiveness, and human-centered impact).

Vignette 1 (V1): Brute-Force Attempt Against User Accounts

In the brute-force scenario, the analytic rule detected the attack and generated an incident, which triggered the automated response workflow to enforce a password change. In the demonstrated run, detection occurred after approximately **11 minutes**, followed by successful execution of the password reset playbook. This result supports both detection validity and automation reliability, demonstrating that SOAR can reduce credential-abuse risk by rapidly initiating corrective action once suspicious authentication patterns are observed (see **Table 3.4** and **Table 3.5**).

Vignette 2 (V2): Data Exfiltration to Unauthorized Cloud Services

For the data exfiltration vignette, an analytic rule identified repeated uploads to an unapproved cloud service and generated an incident once the defined threshold was exceeded. The automation rule then executed the account lockout playbook. In demonstration, the system detected the exfiltration after approximately **7 minutes** and locked the account as expected. This outcome indicates effective containment by reducing the attacker's opportunity to continue exfiltration activity (see **Table 3.3**, **Table 3.4**, and **Figure 3.2**).

Vignette 3 (V3): Compromised Account With Anomalous Login

In the compromised-account vignette, anomalous login behavior (e.g., location-based suspicion in the source implementation) triggered an incident that executed the account lockout playbook. Demonstration showed detection after approximately **6 minutes**, followed by successful lockout. This supports the view that SOAR is particularly well-suited for post-compromise containment where attacker actions become visible through identity and access telemetry (see **Figure 3.3** and **Table 3.5**).

Vignette 4 (V4): Awareness Enhancement Through Notifications

In the malware-prevention vignette, endpoint protection prevented test malware execution and generated a relevant event that was converted into a SIEM incident. The automation rule triggered a SOAR

***Corresponding Author:** Nonye Peter Awurum

playbook that sent an email notification to the affected user. In demonstration, the event was detected after approximately **8 minutes**, and the notification was delivered successfully. This outcome supports the human-centered rationale for immediate feedback following real prevented attacks, differentiating it from simulated awareness exercises (see **Table 3.4** and **Figure 3.2**).

Cross-Scenario Summary of Effectiveness

Across vignettes, the SOAR measures were successful in (i) triggering automated containment actions after incident creation, (ii) reducing reliance on manual analyst intervention for repeatable response steps, and (iii) supporting consistent incident handling within a layered security approach (see **Table 3.5**). The outcomes collectively indicate that automated actions—credential reset, account lockout, and user notification—can reduce exposure after suspected social engineering compromise by shortening response time and limiting attacker dwell time once suspicious behaviors are detected in telemetry (see **Figure 3.3**).

Results Synthesis (Linking Findings to Study Objectives)

The results align with the study's design objectives (see **Table 3.1**) by demonstrating that SOAR playbooks can be implemented as complementary safeguards that reduce the consequences of social engineering incidents through automated incident response. Notably, the demonstrated time-to-response window (minutes rather than hours) underscores the operational value of automation under conditions of skills shortages and increasing attack frequency.

Section 5 discusses the implications of these results, including practical considerations for operational deployment, limitations, and how continuous improvement of detection logic and playbooks can sustain effectiveness against evolving social engineering tactics

DISCUSSION

Interpretation of Findings

This study set out to examine whether SOAR-enabled automated incident response can reduce organizational exposure to social engineering by accelerating containment and standardizing response actions once suspicious activity becomes observable in security telemetry. The results demonstrate that automated playbooks—such as password resets, account lockouts, and user notifications—can be reliably triggered by SIEM-generated incidents and executed within minutes, thereby reducing attacker dwell time and limiting post-compromise impact. Consistent with established incident response thinking, these outcomes primarily strengthen the **detection-and-analysis** and **containment/eradication/recovery** phases by shortening the time between recognizing an anomaly and executing corrective action.

A key insight is that SOAR's value is most pronounced **after** the initial manipulation phase of a social engineering attempt. Early-stage social engineering often occurs without a malicious payload and may not be technically detectable; however, subsequent attacker actions frequently generate observable indicators (e.g., anomalous sign-ins, unusual file transfers, endpoint prevention events). SOAR is well-positioned to convert these signals into rapid response actions that interrupt adversary progression and reduce the consequences of human error. This finding aligns with the broader argument that no single measure prevents all social engineering but modern technologies can reduce risk when deployed as complementary layers within a mature security architecture.

Implications for the Nigerian Financial Sector (Operational and Regulatory Relevance)

For financial institutions operating in regulated environments, the demonstrated SOAR measures have implications beyond technical containment. Automated workflows can enhance **consistency, auditability, and timeliness** of incident handling—properties that are typically expected in financial-sector governance and compliance programs. By generating standardized incident records, preserving playbook execution logs, and documenting response actions (e.g., account lock, credential reset), SOAR can support evidence-based reporting and internal assurance processes.

Additionally, SOAR provides a pragmatic response to persistent **skills shortages** by automating repetitive tasks and enabling security teams to focus on higher-order analysis and decision-making. Importantly, the results reinforce that automation should be viewed as an **amplifier** rather than a replacement for human analysts; SOAR requires skilled personnel for tuning detections, maintaining playbooks, and ensuring that automated actions align with business risk appetite and operational realities.

Why the Approach Works: Linking Vignettes to Controls

The vignette-to-playbook mapping illustrates a practical control strategy: pair **high-likelihood social engineering outcomes** with **low-latency automated containment**. For example:

- **Credential pressure (brute force / credential stuffing)** is addressed by automated password resets, which disrupt unauthorized access attempts and reduce the risk of persistent compromise.
- **Indicators of exfiltration** trigger account lockouts, limiting continued access and potentially curtailing data loss.
- **Anomalous sign-in behavior** triggers immediate containment (account lock), a decisive action that reduces downstream activity such as lateral movement or further credential abuse.
- **Prevented malware events** trigger user notifications, supplying immediate feedback to

***Corresponding Author:** Nonye Peter Awurum

strengthen real-world awareness beyond simulated training.

This mapping operationalizes a "human-centered" posture: rather than expecting perfect user behavior, the security architecture adds safeguards around users and compensates for inevitable errors through rapid and consistent response.

Practical Implementation Considerations

While the results are promising, effective deployment depends on prerequisites and careful governance:

1. **Telemetry readiness and tool integration.** SOAR effectiveness is constrained by the availability and quality of log sources feeding the SIEM (identity, endpoint, cloud, network). Without sufficient telemetry, detection rules may fail to trigger or may generate excessive false positives.
2. **Playbook safety and business impact.** Automated containment (e.g., account lockout) can disrupt legitimate business operations. Organizations should implement approval gates for certain actions, define escalation paths, and apply role-based exceptions for high-privilege or mission-critical accounts.
3. **Continuous improvement lifecycle.** Social engineering tactics evolve; therefore, vignettes, analytic rules, and playbooks should be regularly reviewed and refined. Establishing a lifecycle for tuning and expansion is essential to sustain effectiveness over time.
4. **Cost and maturity alignment.** Operating SIEM/SOAR platforms can be resource-intensive; organizations typically benefit most when they already possess baseline controls and sufficient security maturity to maintain automation and response processes.

These considerations reinforce the conclusion that SOAR is a valuable component within layered defense, but not a standalone solution for social engineering.

Limitations

Several limitations should be acknowledged. First, the demonstration-based evaluation emphasizes functional validation of detections and playbook execution rather than long-term measurement of incident reduction in production environments. Second, SOAR measures address primarily the **post-compromise** stage; the initial psychological manipulation stage remains difficult to prevent with technical controls alone. Third, platform-specific implementations (e.g., Microsoft Sentinel logic apps and rules) may affect generalizability across different SOAR/SIEM stacks, even though the underlying concepts remain portable. Finally, as with all automated systems, false positives and misconfigurations can introduce operational risk, underscoring the need for governance, testing, and staged rollout.

Recommendations and Future Research

Building on these findings, future work should evaluate the comparative effectiveness of **automated vs. manual incident response** under similar conditions, including metrics such as mean time to detect/respond, containment success rates, and downstream loss reduction. Additional vignettes could broaden coverage of social engineering patterns relevant to financial environments (e.g., invoice fraud and BEC-driven payment diversion), while integrating advanced detection approaches such as UEBA and ML-based correlation as part of a hybrid analytic strategy. Finally, research should further explore socio-technical dimensions—how automated containment affects user behavior, trust, and organizational learning—given that social engineering is inherently psychological and organizational as well as technical.

Section 6 provides practical implementation guidance, including steps for operationalizing SIEM analytics, developing additional vignettes and playbooks, and establishing a continuous improvement lifecycle to maintain effectiveness against evolving social engineering threats.

IMPLEMENTATION GUIDANCE

This section provides practical guidance for operationalizing SOAR-enabled automated incident response against social engineering–related threats in financial-sector environments. The guidance is structured around (1) strengthening SIEM analytics, (2) developing additional vignettes and SOAR measures, (3) instituting a continuous improvement lifecycle, and (4) applying risk-based threat modeling to prioritize controls. These recommendations follow the implementation logic and operational considerations emphasized in the base study.

Strengthening SIEM Analytics and Detection Coverage

A SOAR program is only as effective as the detections that trigger it. The base study highlights that SIEM/SOAR automation depends on reliable telemetry and well-designed analytic rules to generate incidents for orchestration. Accordingly, implementation should begin with expanding and tuning SIEM analytics for social engineering–relevant signals.

Recommended actions

1. **Expand data sources feeding the SIEM.** Prioritize identity, endpoint, cloud service, and email security logs because social engineering often manifests in authentication anomalies, endpoint prevention events, and suspicious content delivery.
2. **Enhance correlation logic for SE scenarios.** Implement rules that correlate multiple weak signals (e.g., unusual login + mailbox forwarding rule creation + external file uploads) into higher-confidence incidents.

***Corresponding Author:** Nonye Peter Awurum

3. **Combine traditional rules with anomaly/behavior analytics.** The base study emphasizes that ML/UEBA can complement conventional detections; a hybrid approach improves incident generation quality.
4. **Standardize classification using ATT&CK mappings.** Mapping detections to known techniques supports consistent triage, reporting, and continuous improvement.

Practical output

- A "social engineering detection pack" consisting of tuned analytic rules for: brute-force/credential abuse, suspicious sign-ins, abnormal cloud uploads/exfiltration, and malware prevention events.

Developing Additional Vignettes and SOAR Measures

The base study stresses that effective SOAR requires realistic vignettes (use cases) that reflect the organization's threat landscape and can be tested, refined, and extended over time. In practice, vignettes serve as the bridge between real-world risks and automated playbooks.

Recommended actions

1. **Prioritize new vignettes based on operational risk.** Build scenarios around the most damaging outcomes (e.g., account takeover, fraudulent transactions, ransomware pre-staging, data exfiltration).
2. **Extend beyond the initial four vignettes.** The base study suggests broadening coverage (e.g., web infrastructure attacks, automated blocking, or threat intel actions) as capability matures.
3. **Add playbooks that coordinate multiple controls.** For example, a single incident could trigger: disable account, revoke sessions, isolate endpoint, block IP, and open a ticket—depending on severity and confidence.
4. **Introduce automated notifications to internal/external stakeholders where appropriate.** This can include structured internal escalation and evidence packaging; the base study also notes the possibility of notifying authorities depending on policy.

Examples of "next-step" SOAR measures

- **IOC sharing and enrichment workflows:** automatically enrich indicators and share internally across teams.
- **Automated blocking actions:** block suspicious IPs or domains associated with active campaigns (where supported by infrastructure).
- **Enhanced identity protections:** enforce password reset and lockout combined with user notification and manager escalation for privileged accounts.

Establishing a Continuous Improvement Lifecycle

A central operational message in the base study is that SOAR effectiveness declines if detections and playbooks are not continuously maintained and adapted to evolving threats. Therefore, organizations should formalize a lifecycle that treats SOAR as a living system rather than a one-time deployment.

Recommended lifecycle components

1. **Regular tuning cadence.** Review false positives/negatives, adjust thresholds, and update rules monthly or quarterly depending on incident volume.
2. **Playbook maintenance and testing.** Validate that integrations, permissions, and automated actions still function after system changes (e.g., IAM policy updates).
3. **Lessons-learned integration.** Convert post-incident insights into new detections and refined playbooks to reduce repeat occurrences.
4. **Version control and change governance.** Maintain documentation for playbook logic, escalation conditions, and rollback steps; treat playbooks as controlled operational artifacts.

Deliverable

- A documented **SOAR Continuous Improvement Plan** describing ownership, review schedules, testing procedures, and KPIs (e.g., mean time to respond, playbook success rate).

Threat Modeling and Risk-Based Prioritization

The base study recommends threat modeling to determine which threats are relevant and to prioritize investments accordingly, noting that not all threats apply equally across organizations. Threat modeling helps ensure that SOAR measures focus on the most likely and most damaging scenarios.

Recommended actions

1. **Identify high-impact SE-driven attack paths.** For example: phishing → credential compromise → cloud access → data exfiltration → extortion.
2. **Rank scenarios by likelihood and impact.** Prioritize playbooks that reduce existential or high-frequency risks first.
3. **Map prioritized threats to ATT&CK and controls.** This supports repeatability and structured communication across teams.
4. **Use results to build the vignette backlog.** The prioritized list becomes the roadmap for new detections and response automation.

Operational Readiness and Governance

The base study notes that SOAR requires both skilled resources and economic justification, and that benefits are strongest in organizations with sufficient cybersecurity maturity. To ensure safe adoption:

Recommended governance safeguards

- **Define containment authority levels.** Some actions (e.g., disabling executives' accounts) may require approval gates.
- **Implement a "safe mode" rollout.** Start with alert enrichment and notifications, then progress to active containment once false positives are controlled.
- **Maintain audit-ready evidence.** Store incident and playbook run logs for traceability and compliance support.
- **Assess cost and value.** Consider operational overhead, log ingestion costs, and staffing needs; return on security investment can be difficult to quantify but should be considered in relation to potential breach impact.

Section 7 concludes the study by summarizing contributions, limitations, and directions for future research—particularly the comparative value of automated versus manual incident response and the extension of SOAR measures to additional social engineering scenarios.

CONCLUSION

This study examined how **SOAR-enabled automated incident response** can strengthen defenses against **social engineering–related threats** in financial-sector environments by reducing the consequences of human error after suspicious activity becomes observable in security telemetry. The findings indicate that automation playbooks—such as **account lockdown**, **forced password resets**, and **user notifications following prevented malware events**—can provide a responsive layer of control that improves containment and supports consistent incident handling.

A key conclusion is that SOAR's value is strongest in the **post-compromise phase**, where SIEM-detected signals (e.g., brute-force patterns, anomalous logins, exfiltration behaviors, endpoint prevention events) can trigger rapid containment actions. This aligns with the broader understanding that early-stage social engineering is often difficult to detect because it may occur without an identifiable payload; however, subsequent attacker actions typically generate artifacts that can be captured in logs and endpoint telemetry and acted upon through orchestration and automation.

The study also reinforces that SOAR should not be treated as a "silver bullet." Instead, it functions best as a **complementary measure** within a layered, human-centered security architecture that includes awareness, detection engineering, and mature incident response processes. Importantly, given the widely recognized **skills shortage** in cybersecurity, SOAR-driven automation can help reduce analyst workload and improve response consistency—while still requiring skilled personnel for tuning, governance, and continuous improvement.

Contributions. The work contributes (1) a scenario-driven method for translating social engineering risks into actionable detections and playbooks, (2) a practical automation approach anchored in SIEM/SOAR integration and standardized technique classification, and (3) an implementation-oriented pathway that emphasizes continuous improvement and operational feasibility.

LIMITATIONS

Several limitations should be considered when interpreting these findings. First, the evaluation approach emphasizes **demonstration through vignettes** and validation of automated execution paths rather than long-term measurement of incident reduction or financial loss prevention in a live production environment. While vignette-based demonstrations provide strong evidence of technical feasibility and response logic, broader organizational performance impacts require extended observation.

Second, the measures primarily mitigate **post-breach risk** rather than preventing the initial psychological manipulation stage of social engineering. This constraint is consistent with the view that targeted early-stage social engineering may be difficult to detect technically until later attacker behaviors appear in telemetry.

Third, platform and configuration dependencies can limit direct transferability. The base approach relies on SIEM/SOAR capabilities and integrations (e.g., playbooks, automation rules, analytic rules), and specific implementations may vary across vendors and environments; however, the underlying design logic remains portable at the conceptual level.

Finally, operational constraints—such as the cost of log ingestion, infrastructure, and the availability of skilled staff to maintain detections and playbooks—may affect scalability and sustainability. The base study notes that operating SIEM/SOAR systems can involve non-trivial costs and that effective use typically presupposes a degree of cybersecurity maturity and supporting tooling.

FUTURE RESEARCH

Future work should expand evaluation beyond technical demonstrations to include comparative and longitudinal assessments. One priority direction is to test whether **automated incident response** is measurably superior to manual response across metrics such as mean time to respond, containment success, recurrence reduction, and operational workload.

Second, additional social engineering vignettes and automation measures should be developed to broaden coverage of realistic threats and extend the playbook library. The base study emphasizes that

***Corresponding Author:** Nonye Peter Awurum

expanding vignette sets and iteratively refining detections is essential for sustaining effectiveness in a changing threat landscape.

Third, the role of advanced analytics—such as ML/UEBA combined with rule-based detections—should be investigated to improve incident fidelity and reduce false positives, while maintaining transparency and operational control.

Finally, further research should address socio-technical aspects of social engineering and automation, including how automated containment and real-incident user notifications influence employee behavior, risk perception, and organizational learning. Because social engineering is inherently psychological and organizational as well as technical, studies that integrate these dimensions can provide a richer understanding of sustainable, human-centered defense.

REFERENCES

1. Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science, 10*(5), 1–3. https://doi.org/10.26483/ijarcs.v10i5.6476
2. Blake, S., Andy, A., Doug, M., Kathryn, N., Adam, P., & Cody, T. (2020). *MITRE ATT&CK: Design and philosophy*. MITRE. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
3. Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2022). *Test. SOAR Tools Use, 1*(1), 1–37. http://arxiv.org/abs/2208.06075
4. Central Bank of Nigeria. (2024, May). *Risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks*. https://www.cbn.gov.ng/Out/2024/BSD/CBN%20Risk-Based%20Cybersecurity%20Framework%20for%20DMBs%20and%20PSBs_2024.pdf [cbn.gov.ng]
5. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). Overview of social engineering attacks on social networks. *Procedia Computer Science, 198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302
6. Chiconski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2
7. Coffey, J. W. (2017). Ameliorating sources of human error in cybersecurity: Technological and human-centered approaches. In *IMCIC 2017—8th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings* (pp. 85–88).
8. Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security, 69*, 18–34. https://doi.org/10.1016/j.cose.2016.12.013
9. ENISA. (2022). *What is "Social Engineering"?* https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering
10. Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667–4679. https://doi.org/10.1002/sec.1657
11. Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023* [PDF]. KPMG. https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023.pdf
12. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cybersecurity culture framework. *Sensors, 21*(9). https://doi.org/10.3390/s21093267
13. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008
14. Islam, C., Babar, M. A., & Nepal, S. (2020). Architecture-centric support for integrating security tools in a security orchestration platform. In *Lecture Notes in Computer Science* (Vol. 12292, pp. 165–181). https://doi.org/10.1007/978-3-030-58923-3_11
15. Kinyua, J., & Awuah, L. (2021). AI/ML in security orchestration, automation and response: Future research directions. *Intelligent Automation & Soft Computing, 28*(2), 527–545. https://doi.org/10.32604/iasc.2021.016240
16. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
17. Mayring, P. (2022). *Qualitative Inhaltsanalyse, Grundlagen und Techniken* (13th ed.). Beltz.
18. Mitnick, K., & Simon, W. (2006). *Die Kunst der Täuschung* (1st ed.). mitp.
19. Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004
20. Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security, 55*, 114–127. https://doi.org/10.1016/j.cose.2015.09.001
21. Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent

resource-based analysis. *International Journal of Information Management, 59*, 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

22. Odeh, N. A., Eleyan, D., & Eleyan, A. (2021). A survey of social engineering attacks: Detection and prevention tools. *Journal of Theoretical and Applied Information Technology, 99*(18), 4375–4386.
23. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
24. Pratt, M. (2021). *What is security awareness training?* TechTarget. https://www.techtarget.com/searchsecurity/definition/security-awareness-training
25. Ross, R., Pillitteri, V., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2). https://doi.org/10.6028/NIST.SP.800-160v2r1
26. Sridharan, A., & Kanchana, V. (2022). SIEM integration with SOAR. In *2022 International Conference on Futuristic Technologies (INCOFT)* (pp. 1–6). https://doi.org/10.1109/INCOFT55651.2022.10094537
27. Venable, J. R., Pries-Heje, J., & Baskerville, R. (2017). Choosing a design science research methodology. In *Proceedings of the 28th Australasian Conference on Information Systems (ACIS 2017).*
28. Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports, 4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126

***Corresponding Author:** Nonye Peter Awurum