MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

SANS And NIST Incident Response Frameworks and Incident Report for Twitter and Marriott Data Breaches

Lab Assignment 4
Incidence Reports in NIST and SANS formats

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

April 3, 2025

Contents

Chapter 1

SANS Incident Response Framework

1.1 History and Origins

Developed by the **SANS Institute** in the late 1990s, this framework emerged from one of the world's largest cybersecurity training and certification organizations. It was designed to provide a standardized approach for handling security incidents, with a focus on **practical, operational guidance** for security teams[1][2].

1.2 Primary Use Cases

- Widely adopted by organizations with mature security operations centers (SOCs)
- Preferred in industries requiring strict compliance with security-focused standards
- Used by incident responders needing granular, phase-specific guidance[8][10]

1.3 Phases and Recommendations

The framework consists of six distinct phases:

1. **Preparation**: Develop IR plans, conduct risk assessments, and establish CSIRT teams
2. **Identification**: Monitor systems for deviations from baseline activity
3. **Containment**: Implement short-term (network isolation) and long-term (system hardening) measures
4. **Eradication**: Remove malware and attack artifacts
5. **Recovery**: Restore systems with validation testing
6. **Lessons Learned**: Conduct post-incident reviews and update playbooks[2][5]

1.4 Key Features

- Provides detailed checklists for Windows/UNIX systems
- Emphasizes **triage and prioritization** during detection

- Separates containment, eradication, and recovery into discrete phases[7][9]

Chapter 2

NIST Incident Response Framework

2.1 History and Origins

Created by the **National Institute of Standards and Technology (NIST)** through Special Publication 800-61. First published in 2004 and regularly updated, it serves as a **government-endorsed standard** for cybersecurity incident handling[3][6].

2.2 Primary Use Cases

- Mandatory for U.S. federal agencies
- Adopted voluntarily by private sector organizations
- Used in critical infrastructure protection (energy, finance, healthcare)[3][10]

2.3 Phases and Recommendations

Four-phase structure outlined in NIST SP 800-61:

1. **Preparation**: Establish IR policies and threat intelligence capabilities
2. **Detection & Analysis**: Implement SIEM tools and escalation procedures
3. **Containment, Eradication & Recovery**: Combined workflow for simultaneous threat mitigation
4. **Post-Incident Activity**: Documentation and process improvement[3][6]

2.4 Key Features

- Focuses on **system monitoring and escalation procedures**
- Provides three organizational models (central/distributed/coordinated teams)
- Emphasizes continuous process improvement cycles[6][8]

Chapter 3

Comparison of SANS and NIST Incident Response Frameworks

3.1 Structural Differences

- The **SANS framework** consists of six distinct phases, clearly separating containment, eradication, and recovery, whereas **NIST condenses these into a single phase**.

- NIST's four-phase structure focuses more on broad incident response and process improvement, whereas SANS provides **granular, operational guidance**.

3.2 Applicability and Use Cases

- **SANS** is widely used in SOC environments and industries with high security requirements (e.g., finance, healthcare, government contractors).

- **NIST** is a **regulatory standard** for U.S. federal agencies and a preferred model for organizations requiring a structured, compliance-focused approach.

3.3 Incident Handling Approach

- **SANS** prioritizes immediate operational response and containment strategies, making it ideal for SOCs and organizations needing rapid triage.

- **NIST** emphasizes a cyclical approach with continuous monitoring and learning, making it useful for enterprises focusing on long-term security improvements.

3.4 Flexibility and Adaptability

- **SANS** offers prescriptive guidance, which is beneficial for structured incident response but may require adaptation for specific organizations.

- **NIST** is highly adaptable due to its broad guidelines, allowing organizations to integrate the framework with existing processes.

3.5 Conclusion

Both frameworks provide robust methodologies for incident response but cater to different organizational needs. Organizations should choose the appropriate framework based on their regulatory environment, security maturity, and operational priorities. A hybrid approach leveraging both frameworks can enhance overall cybersecurity resilience.

Chapter 4

SANS Incidence Report for The Marriott data breach

4.1 Introduction

The Marriott data breach stands as one of the largest and most significant cybersecurity incidents in the hospitality industry. This report analyzes the incident using the SANS Incident Response Framework to provide insights into what happened and lessons that can be learned.

4.2 What Happened?

Attackers compromised Starwood's reservation system in 2014 through a web shell installation on an internal application server, remaining undetected even after Marriott acquired Starwood in 2016. The breach exposed personal information of approximately 339 million guests worldwide, including names, contact details, passport numbers, and payment card information. The intrusion was finally discovered in September 2018, nearly four years after initial compromise.

4.3 SANS Response

4.3.1 Preparation

The preparation phase reveals significant security gaps that contributed to the breach's severity:

- **Insufficient due diligence:** When Marriott acquired Starwood in 2016, it inherited already compromised systems as adequate security assessment was not performed during merger and acquisition activities.

- **Inadequate security controls:** Starwood properties were using outdated versions of Windows Server and had remote desk protocol (RDP) ports open to the internet.

- **Poor monitoring infrastructure:** Security alerts were configured only for specific sensitive database tables containing payment card data, rather than comprehensive monitoring across all personal data repositories.

- **Inconsistent encryption practices:** Marriott applied encryption only to passport numbers and payment card data, leaving other personal information unprotected. Additionally, a script for decrypting AES-128 bit encrypted entries was compromised, indicating poor cryptographic key management.

4.3.2 Identification

The breach was finally identified after operating undetected for four years:

- On September 7, 2018, an attacker ran a database query to count records in the `Guest_Master_Profile` table. This unusual activity triggered an alert from Guardium, the database monitoring tool installed on the server.
- The security team observed this alert and notified Marriott's IT team on September 8, 2018.
- This discovery occurred a full four years after the initial breach, highlighting the sophisticated and persistent nature of the attack.

4.3.3 Containment

Once the breach was identified, Marriott took several immediate steps to contain the damage:

- Marriott initiated its incident response plan on September 9-10, 2018, deploying real-time endpoint monitoring and forensic tools across approximately 70,000 systems.
- The security team identified and contained the Remote Access Trojan (RAT) malware that had provided persistent access to the attackers.
- Command and Control (C&C) IP addresses used by the attackers were blocked at the network level to prevent further communication.
- Marriott consulted forensic specialists and reported the incident to law enforcement officials to support the investigation.

4.3.4 Eradication

The eradication phase involved identifying and removing all malicious components:

- Endpoint monitoring tools helped discover previously undetected attacker activity, including unauthorized use of credentials, presence of RAT malware, C&C communications, and use of credential-harvesting tools like Mimikatz.
- Investigators discovered encrypted and deleted database dump (.dmp) files that had been created between April 2015 and May 2016 with the intention of exfiltrating personal data.
- After identifying the attack vectors, security teams removed malicious software and restored affected systems to secure configurations, although specific details of this process were not fully disclosed in public reports.

4.3.5 Recovery

The recovery phase focused on notification, assessment, and remediation:

- On October 29, 2018, Marriott contacted the FBI, and on November 22, 2018, notified the UK Information Commissioner's Office (ICO) of the data breach.

- On November 30, 2018, Marriott publicly disclosed the breach, revealing initially that up to 500 million guest records were potentially compromised (later revised to 339 million).
- Upon decrypting the exfiltrated data, Marriott determined that it contained sensitive personal information including names, emails, dates of birth, mailing addresses, passport numbers, and payment card details.
- In response to the breach, the ICO initially announced plans to fine Marriott £99.2 million, which was later reduced to £18.4 million (approximately $23.8 million).

4.4 Lessons Learned

The Marriott breach offers several critical lessons for organizations:

- **Enhanced M&A due diligence:** Organizations should conduct thorough cybersecurity assessments during acquisitions, including compromise assessments to detect existing breaches before integration.
- **Comprehensive monitoring:** Monitoring should cover all systems containing personal data, not just those with payment information. Adequate logging of user actions and database activities is essential.
- **System hardening:** Critical systems require proper hardening, including secure configurations and whitelisting to prevent installation and execution of unauthorized software.
- **Consistent data protection:** All personal data should be protected with appropriate encryption, not just selected fields deemed most sensitive.
- **Privileged account monitoring:** Enhanced monitoring of privileged accounts is necessary to detect and respond to potential abuse, even when multi-factor authentication is implemented.

4.5 Conclusion

The Marriott data breach exemplifies the challenges organizations face with cybersecurity during mergers and acquisitions. The four-year gap between initial compromise and detection demonstrates the persistence of sophisticated attackers and the critical importance of comprehensive security monitoring. By implementing the lessons learned from this incident, organizations can better protect themselves against similar breaches and minimize the impact when incidents do occur.

This case highlights that cybersecurity must be a fundamental consideration during corporate acquisitions, not an afterthought. Technical security controls must be paired with effective processes for detection, response, and recovery to provide comprehensive protection for sensitive customer data.

Chapter 5

NIST Incident Response Report for Twitter Data Breach (2020)

5.1 Introduction

The Twitter data breach of July 15, 2020, involved a coordinated social engineering attack targeting employees with access to internal administrative tools. This led to the compromise of 130 accounts, including those of high-profile individuals and organizations, and was used to promote a cryptocurrency scam. This report analyzes the incident using the NIST Incident Response Framework, as outlined in Special Publication 800-61 Rev. 2.

5.2 Preparation

The preparation phase revealed significant gaps in Twitter's cybersecurity readiness:

- **Policy & Planning:** Twitter lacked adequate policies to mitigate insider threats and did not enforce strict access controls for its administrative tools. Additionally, there was no Chief Information Security Officer (CISO) at the time of the breach, leading to a lack of centralized security oversight.

- **Incident Response Team (IRT):** While Twitter had an incident response team, the delayed response to the attack suggests inefficiencies in their processes for rapid containment and mitigation.

- **Tools & Resources:** The administrative tools used by employees were insufficiently protected, allowing attackers to bypass two-factor authentication (2FA) through social engineering. Monitoring systems also failed to detect unusual activity promptly.

- **Training & Awareness:** Employees were targeted through phone spear-phishing attacks, exploiting their lack of awareness about social engineering techniques. This highlights inadequate training on recognizing and responding to phishing attempts.

- **Threat Intelligence:** There was no evidence that Twitter actively monitored for emerging threats or conducted regular security audits to identify vulnerabilities in its internal processes.

5.3 Detection & Analysis

The detection and analysis phase exposed delays in identifying and assessing the breach:

- **Indicators of Compromise (IoCs):** The attackers gained access to internal tools by tricking employees into providing credentials via a fake VPN login page. This activity went undetected until the attackers began tweeting from compromised accounts.
- **Incident Categorization:** The breach involved unauthorized access to high-profile accounts and misuse of these accounts for a cryptocurrency scam. It also included unauthorized downloads of sensitive account data.
- **Impact Analysis:**
  - 130 accounts were compromised.
  - 45 accounts were used to tweet scam messages.
  - 36 accounts had their Direct Messages (DMs) accessed.
  - Data from 8 accounts were downloaded using Twitter's "Your Twitter Data" tool.
  - Over $118,000 in Bitcoin was stolen from victims.
- **Forensic Analysis:** Investigators determined that attackers used social engineering techniques to gain access to internal systems. They exploited weaknesses in multi-factor authentication (MFA) processes and leveraged employee credentials to escalate privileges.
- **Incident Reporting:** Twitter publicly acknowledged the breach within hours but did not provide detailed information until later investigations were completed. Law enforcement agencies were notified promptly.

5.4 Containment, Eradication, and Recovery

Twitter took several steps to contain and recover from the breach:

- **Short-Term Containment:**
  - Access to compromised accounts was locked down.
  - Functionality for verified accounts was temporarily restricted, preventing them from tweeting or resetting passwords.
  - Internal administrative tools were disabled while the investigation was underway.
- **Long-Term Containment:**
  - Employee access to administrative tools was significantly restricted.
  - Additional security measures were implemented for high-profile accounts, including enhanced MFA protections.
- **Eradication:**
  - Credentials obtained through phishing attacks were revoked.
  - Administrative tools were audited and secured against further exploitation.

  - Processes for employee authentication were updated to prevent similar attacks in the future.

- **Recovery:**
  - Affected accounts were restored after verification of ownership.
  - Users whose data had been downloaded or accessed were notified directly.
  - Cryptocurrency exchanges like Coinbase helped block further transactions, preventing an additional $1.5 million in potential losses.

- **Post-Incident Monitoring:** Enhanced monitoring systems were deployed to detect unusual activity on administrative tools and high-profile accounts.

5.5 Post-Incident Activity (Lessons Learned)

The post-incident phase focused on addressing security gaps and improving resilience:

- **Incident Debriefing:** Twitter conducted an internal investigation and collaborated with law enforcement agencies to understand the full scope of the attack. Findings revealed systemic weaknesses in employee training and tool security.

- **Root Cause Analysis:**
  - The primary cause was a lack of robust protections against social engineering attacks targeting employees.
  - Inadequate access controls allowed attackers to escalate privileges once initial credentials were compromised.

- **Policy and Control Updates:**
  - Access controls for administrative tools were tightened.
  - Security policies were updated, emphasizing insider threat prevention and stronger MFA mechanisms.
  - A new CISO was hired shortly after the incident to oversee cybersecurity improvements.

- **Training and Awareness:** Employees received enhanced training on recognizing phishing attempts and responding appropriately. Regular simulation exercises were introduced to test employee readiness against social engineering attacks.

- **Report Documentation:** Detailed records of the incident were maintained for compliance purposes and shared with stakeholders as part of transparency efforts. Lessons learned were documented and shared with other organizations as part of broader industry awareness initiatives.

Conclusion

The Twitter data breach underscores the critical importance of securing internal systems, training employees against social engineering threats, and implementing robust access controls. By addressing these gaps through policy updates, improved training programs, and enhanced monitoring systems, organizations can better protect themselves against similar incidents in the future.