Building Correlation Rules and Playbooks Using the MITRE ATT&CK Framework

Gili Levy  
Email: gililevy1993@gmail.com  
Published: October 05, 2024

# Abstract

This article provides a comprehensive guide on building correlation rules and playbooks using the **MITRE ATT&CK** framework for web applications and MySQL databases. It explains the fundamentals of the **MITRE ATT&CK** framework and offers step-by-step instructions for creating correlation rules to detect security incidents such as **SQL** injection, abnormal database query execution, and failed login attempts. Additionally, the article presents a playbook for responding to detected threats and simulating attacks using tools like **SQLMap** and **Python**. By utilizing the **MITRE ATT&CK** framework, organizations can enhance their detection mechanisms, automate response processes, and improve overall security defenses.

Table of Contents

[Abstract 1](#_Toc179061063)

[1. Introduction 2](#_Toc179061064)

[2. Literature Review 3](#_Toc179061065)

[3. Correlation Rules and Playbooks using the MITRE ATT&CK Framework 4](#_Toc179061066)

[What is the MITRE ATT&CK Framework? 4](#_Toc179061067)

[3.2 Correlation Rules: Linking Logs to ATT&CK Techniques 5](#_Toc179061068)

[3.3 Steps to Build Correlation Rules Using the MITRE ATT&CK Framework 5](#_Toc179061069)

[Correlation Rules for Web Applications and MySQL Databases 6](#_Toc179061070)

[Rule 1: SQL Injection Detection in Web Application Logs 6](#_Toc179061071)

[Rule 2: Abnormal Database Query Execution 6](#_Toc179061072)

[Rule 3: Failed Login Attempts and Privilege Escalation Attempts 6](#_Toc179061073)

[Rule 4: Data Exfiltration Detection 6](#_Toc179061074)

[Playbook for Responding to Detected Threats 7](#_Toc179061075)

[Playbook: Automated Response for SQL Injection and Data Exfiltration 7](#_Toc179061076)

[Step 1: Alert and Notification 7](#_Toc179061077)

[Step 2: Containment 7](#_Toc179061078)

[Step 3: Investigation 7](#_Toc179061079)

[Step 4: Remediation 7](#_Toc179061080)

[Step 5: Post-Incident Reporting and Lessons Learned 7](#_Toc179061081)

# Introduction

In today's rapidly evolving digital landscape, organizations rely heavily on information and technology to drive innovation and maintain competitive advantage. However, this dependence exposes them to a range of security risks, including data breaches, prolonged service disruptions, and cyberattacks, which can significantly impact business continuity. To mitigate these risks, it is crucial to implement a comprehensive information security strategy.

One effective approach to strengthening detection and response mechanisms is by leveraging the **MITRE ATT&CK** framework, a widely adopted knowledge base of adversarial tactics and techniques. While this framework provides valuable insights, transforming those insights into actionable security controls requires a structured, methodical approach.

This article provides both strategic and practical guidance on building correlation rules and automated playbooks for web applications and **MySQL** databases, using the **MITRE ATT&CK** framework. By integrating this framework, organizations can enhance their detection capabilities and automate their incident response processes, ultimately improving their overall security posture.

# Literature Review

In the field of cybersecurity, the **MITRE ATT&CK** framework has emerged as a leading model for understanding adversary behavior through the categorization of tactics and techniques. This framework has been widely adopted in the cybersecurity community for threat hunting, incident response, and security operations. By mapping attack behavior, organizations can develop tailored defense strategies and improve security defenses by utilizing correlation rules within SIEM systems, such as **IBM QRadar** and **Splunk**.

# Correlation Rules and Playbooks using the MITRE ATT&CK Framework

## What is the MITRE ATT&CK Framework?

The **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It covers multiple attack vectors, including enterprise IT environments, cloud environments, mobile platforms, and industrial control systems (ICS).

The framework is structured around adversarial behaviors, providing detailed descriptions of each tactic (the "why" of an attack) and technique (the "how" of an attack). This structure allows security teams to understand the lifecycle of an attack and build more robust defense mechanisms.

**The Structure of MITRE ATT&CK**

1. **Tactics:** These represent the adversary's objectives during various stages of an attack. Tactics define **why** an action is being taken. Examples include:
   1. **Initial Access**: Techniques used by attackers to gain access to a network (e.g., phishing or exploiting vulnerabilities).
   2. **Privilege Escalation**: The process attackers use to gain elevated permissions on a compromised system.
   3. **Data Exfiltration**: Techniques used to steal data from the victim’s network.
2. **Techniques**: Techniques describe **how** adversaries achieve their objectives (tactics). Each tactic is further broken down into specific techniques. For instance:
   * 1. **T1566 - Phishing**: Sending emails to trick users into revealing credentials or executing malicious files.
     2. **T1078 - Valid Accounts**: Using stolen or otherwise obtained valid credentials to access systems and move laterally within the network.
3. **Sub-techniques**: MITRE also defines sub-techniques that provide more granular details on how a particular technique is executed. For example, under the **Phishing (T1566)** technique, there are sub-techniques like **Spearphishing Link (T1566.001)** and **Spearphishing Attachment (T1566.002)**.  
     
   By aligning detection, response, and prevention strategies with **MITRE ATT&CK**, organizations can:
4. Improve Detection: Use the knowledge of known attack techniques to monitor for specific behaviors in log data.
5. Perform Threat Hunting: Proactively search for indicators of adversary activity using the techniques from MITRE ATT&CK.
6. Strengthen Defenses: Identify gaps in defenses and improve overall security posture by focusing on critical attack techniques relevant to the organization.

The framework provides a blueprint for structuring an organization’s defense mechanisms around known adversarial behaviors, offering a systematic approach to understanding the full lifecycle of an attack.

## 3.2 Correlation Rules: Linking Logs to ATT&CK Techniques

Correlation rules are predefined logic that security information and event management (**SIEM**) systems use to detect potential threats by analyzing log data across various sources. These rules enable security analysts to automatically identify patterns in log data that correspond to specific attack techniques or behaviors.

## 3.3 Steps to Build Correlation Rules Using the MITRE ATT&CK Framework

1. **Understand the Attack Techniques:** Familiarize yourself with common attack techniques relevant to your organization’s environment, such as credential access, privilege escalation, lateral movement, and data exfiltration.
2. **Identify Relevant Data Sources**: Key data sources may include logs from endpoints, network traffic, authentication systems, and any other security devices or applications deployed in your organization.
3. **Write the Correlation Rule:** Using your **SIEM**, define correlation rules that detect patterns indicative of malicious activities, such as suspicious logins, unauthorized access attempts, or abnormal data transfers.
4. **Use ATT&CK Mappings in SIEM**: Many modern **SIEM** tools, such as **IBM QRadar** or **Splunk**, offer built-in mappings to the **MITRE ATT&CK** framework, allowing you to easily map observed activities to known adversarial tactics and techniques for more effective detection.

## Correlation Rules for Web Applications and MySQL Databases

### Rule 1: SQL Injection Detection in Web Application Logs

Trigger Conditions:  
- The web application receives multiple requests containing SQL keywords such as: `SELECT`, `UNION`, `DROP`, `INSERT`, `OR 1=1`, etc., from the same IP address or user within a short time period.  
- The web server responds with abnormal HTTP status codes (e.g., 500, 503, or errors showing SQL syntax).

### Rule 2: Abnormal Database Query Execution

Trigger Conditions:

* Unusual query patterns in the MySQL logs, such as:
* Large `SELECT` or `UNION` queries that may indicate data dumping.
* Queries containing typical SQL injection patterns.
* Abnormal access to tables containing sensitive data.

### Rule 3: Failed Login Attempts and Privilege Escalation Attempts

Trigger Conditions:

* Multiple failed logins attempt to the MySQL database or web application, followed by a successful login.
* Sudden privilege escalation for a user or a non-admin user attempting privileged actions.

### Rule 4: Data Exfiltration Detection

**Trigger Conditions:**

* Large data retrieval queries (e.g., `SELECT \* FROM sensitive\_table`) and/or abnormally large outbound traffic from the web server or MySQL database.

# Playbook for Responding to Detected Threats

## Playbook: Automated Response for SQL Injection and Data Exfiltration

### Step 1: Alert and Notification

* **Trigger**: SQL Injection or Data Exfiltration rule is activated.
* **Action**:
  + Generate a high-priority alert within the **SIEM** system.
  + Notify the **SOC** team via email or Slack with details of the alert (including affected systems, source IP addresses, and suspicious queries).

### Step 2: Containment

* **Action 1:** Automatically block the suspicious IP address at the network firewall or web application firewall (WAF).
* **Action 2:** Isolate the affected database or web server from the network to prevent further malicious activity or data exfiltration.
* **Action 3:** Limit the affected user's access to the MySQL database or application until the investigation is complete.

### Step 3: Investigation

* **Action 1:** Review the web application and database logs for the specific SQL injection attack patterns and associated queries that triggered the alert.
* **Action 2:** Check network traffic logs for any signs of large outbound data transfers (possible data exfiltration).
* **Action 3:** Use forensic tools to capture a snapshot of the compromised systems for further analysis.
* **Action 4:** Correlate the attack with other ATT&CK techniques used by known adversary groups that could be targeting your web application.

### Step 4: Remediation

- Action 1: Patch any discovered SQL injection vulnerabilities in the web application codebase or database.  
- Action 2: Reset compromised credentials or enforce multi-factor authentication (MFA) for affected accounts.  
- Action 3: If sensitive data has been exfiltrated, inform relevant stakeholders and initiate appropriate data breach protocols.

### Step 5: Post-Incident Reporting and Lessons Learned

- Action 1: Generate a detailed incident report summarizing:  
 - The attack vectors, techniques used, and systems affected.  
 - Steps taken to mitigate the attack and prevent future occurrences.  
- Action 2: Hold a post-incident review session with the SOC and development teams to:  
 - Identify gaps in monitoring, logging, or detection capabilities.  
 - Update or create new correlation rules based on lessons learned.  
- Action 3: Implement longer-term defenses, such as more robust web application firewall (WAF) rules and periodic database integrity checks.

**Conclusion**

The MITRE ATT&CK framework offers a comprehensive structure to understand adversarial behaviors in cybersecurity. By leveraging its tactics and techniques, security teams can build more robust detection mechanisms, respond to incidents more effectively, and continuously improve their defenses.

This article has demonstrated how to construct correlation rules that align with MITRE ATT&CK techniques, particularly for securing web applications and MySQL databases against SQL injections and data exfiltration attempts. In conjunction with these correlation rules, playbooks offer a structured response to contain, investigate, and remediate potential attacks.

By incorporating MITRE ATT&CK into both detection and response workflows, organizations can significantly enhance their visibility into adversarial activity and reduce the response time to active threats. This proactive approach helps mitigate damage and provides an opportunity for continuous improvement in the overall security posture.

**References**

1. MITRE ATT&CK Framework: https://attack.mitre.org

2. SQLMap Project: https://sqlmap.org

3. IBM QRadar: Correlation Rule and Playbook Integration with MITRE ATT&CK

4. OWASP Foundation: https://owasp.org

5. ISO/IEC 27001: Information Security Management System