AMPCUS CYBER
Zero Trust Compliance Service Provider

A STRATEGIC APPROACH TO BUILDING EFFECTIVE USE CASES

www.ampcuscyber.com

Introduction:
The Role of Use Cases in Cybersecurity

In cybersecurity, use cases serve as the foundation for proactive threat detection, incident response, and compliance monitoring. By defining scenarios that reflect real-world threats, organizations can align their cybersecurity strategies with operational needs, minimizing risks and improving resilience.

Why Use Cases Matter:

- Focus security operations on actionable and relevant threats.
- Enhance the efficiency of tools like SIEMS, SOARS, and MDR solutions.
- Bridge the gap between business objectives and technical security controls.

According to a 2024 study by Gartner, organizations that leverage tailored use cases in their security operations saw a 28% improvement in threat detection accuracy and a 40% reduction in false positives. This white paper outlines a systematic approach to developing, refining, and operationalizing cybersecurity use cases to achieve robust defense mechanisms.

Defining a Cybersecurity Use Case

A cybersecurity use case is a documented scenario that describes a specific threat, its detection mechanism, and the response plan. It includes:

- Threat Description: What malicious activity is being addressed?
- Detection Logic: How will the threat be identified?
- Response Action: What steps will be taken to mitigate the threat?

Approach to Writing Effective Use Cases

Developing a strong use case requires a clear understanding of the threat landscape, organizational priorities, and available tools.

The following approach ensures comprehensive and actionable use cases:

1. Identify Business and Security Objectives

- Understand the organization's critical assets and operations.
- Align the use case with business goals (e.g., protecting customer data, ensuring uptime).

Checklist:

- What are the organization's top cybersecurity concerns?
- Which regulations or standards must the organization comply with?
- What incidents would have the greatest operational or financial impact?

2. Leverage Threat Intelligence

Incorporate insights from internal logs and external threat intelligence to address relevant and emerging threats.

Key Considerations:
Industry-specific threats (e.g., ransomware in healthcare).
Geopolitical risks (e.g., state-sponsored attacks).
Historical incidents within the organization.

Stat Insight:
A 2024 Ponemon Institute report highlights that integrating threat intelligence into use cases increases detection accuracy by 45%.

3. Use a Structured Framework

Adopt a standardized template to ensure consistency across use cases.
Here's a suggested format:

Field	Description
Use Case ID	**Unique identifier for tracking and updates.**
Objective	**The goal of the use case (e.g., detect ransomware activity)**
Threat Scenario	**Description of the threat actor, method, and target**
Data Sources	**Logs, tools, or feeds needed to detect the threat.**
Detection Logic	**Correlation rules, thresholds, or ML algorithms to use.**
Response Plan	**Automated or manual actions for containment and remediation.**
Testing Procedure	**Steps to validate the effectiveness of the use case.**

4. Collaborate Across Teams

Engage multiple stakeholders, including:

- **Security Analysts:** To provide insights into current gaps and pain points.
- **IT Teams:** To ensure feasibility within existing infrastructure.
- **Compliance Officers:** To align with regulatory requirements.

Pro Tip: Regular cross-functional workshops can identify blind spots and improve coverage.

5. Focus on Metrics and Continuous Improvement

Define KPIs to measure the use case's effectiveness, such as:

- **Detection Rate:** Percentage of incidents accurately flagged.
- **False Positive Rate:** Ratio of incorrect alerts to total alerts.
- **MTTD (Mean Time to Detect):** Time taken to identify a threat.

6. Test and Validate

Before deploying, test the use case in a controlled environment to ensure accuracy and efficiency.

Validation Steps:

- Simulate scenarios using historical data or red team exercises.
- Assess the performance of detection logic against known threats.
- Refine thresholds or response steps based on testing results.

7. Operationalize the Use Case

Once validated, integrate the use case into the security stack:

- Deploy detection logic into the SIEM or EDR system.
- Automate response workflows using SOAR platforms.
- Train analysts on identifying and managing alerts triggered by the use case.

Example Use Case: Ransomware Attack Detection

- **Objective:** Detect early signs of ransomware activity to prevent encryption of files and reduce downtime.

- **Threat Scenario:** A malicious actor gains access to an endpoint or network and initiates ransomware encryption. Indicators of such an attack include:

    - Bulk file modifications within a short timeframe.
    - High CPU or disk utilization by unrecognized processes.
    - Connections to known ransomware command-and-control (C2) servers.

- **Detection Logic:** Monitor for:
    - High frequency of file write operations or renaming (e.g., encrypted).
    - Unauthorized processes consume excessive resources.
    - Sudden spikes in outbound network traffic or communication with suspicious domains.

- **Data Sources:** Endpoint logs, file server logs, SIEM, and threat intelligence feeds.

- **Response Plan:**
    - Isolate the affected endpoint from the network.
    - Terminate suspicious processes and investigate payloads.
    - Notify the security team and stakeholders.
    - Recover encrypted files from backups if necessary.

Testing Procedure: Use a ransomware simulation tool to test detection thresholds and validate the response workflow.

Common Challenges and Solutions

Common Challenges and Solutions

Challenge: Overly generic use cases leading to alert fatigue.
Solution: Focus on specific threats relevant to your environment.

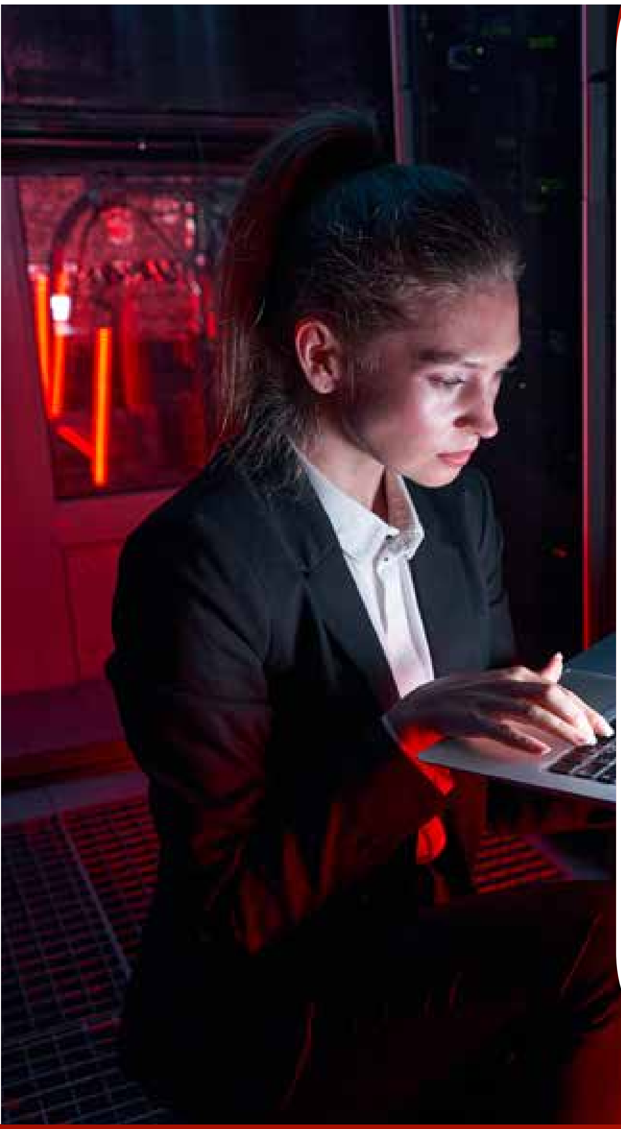
Challenge: Lack of data to build detection logic.
Solution: Integrate diverse data sources, such as DNS logs, endpoint telemetry, and user activity.

Challenge: Rapidly evolving threat landscape.
Solution: Regularly review and update use cases based on the latest threat intelligence.

The Impact of Well-Crafted Use Cases

Organizations that adopt a structured approach to writing use case reports:

- **Reduced Dwell Time:** A 2024 report by IBM X-Force found that tailored use cases helped reduce attacker dwell time by 37%.
- **Improved Analyst Productivity:** Streamlined workflows enable analysts to focus on high-value tasks, increasing productivity by 50%.
- **Stronger Compliance:** Automated use cases ensure continuous monitoring of regulatory requirements, reducing audit findings by 42%.



> “Effective use cases transform a reactive SOC into a proactive threat management powerhouse. It’s all about turning data into actionable insights.”
>
> - John Smith, Cybersecurity Advisor, SANS Institute

Conclusion

A robust cybersecurity posture requires the continuous development and refinement of use cases. By aligning security goals with business needs, leveraging threat intelligence, and adopting a structured approach, organizations can achieve operational efficiency and enhanced resilience against evolving threats.

Investing time in crafting high-quality use cases today will yield significant returns in the form of reduced risk, better compliance, and streamlined operations tomorrow.

Authors

Sujay Mendon, Kavita Konar