SOC Use Cases

Use case life cycle

It is very necessary to optimize and review the test cases so that there is no blind spot left and no overlapping is there. This will increase the optimization

Steps:

1. Objective
   A. Why do we need test case
   B. Gives overview of detection capabilities

2. Threat
   A. What do we want to defend against
   B. Supports Why use case has been created

3. Stakeholders
   A. analysts involved in detecting threats and responding to incidents

4. Data Reqs.
   A. Flow/Endpoint Data sources that are required to be able to detect our Threat

5. Logic
6. Testing
   A. Is Logic Reproducible
   B. Key to validate Rules
   C. Should be first test in QA

7. Priority
   A. Provide Guidance to SOC Analyst
   B. Depends upon the policies and business requirements
8. Output

Example:

Admin credentials abuse

1. Objective : Monitor Unusual access to admin account
2. Threat : Attacker Lateral Movement and use of Admin accounts
3. Stakeholder: SOC Analyst
4. Data Req.: Window Server
5. Logic : Login Out of working hrs/
6. Testing : Conduct test with admin out of working hrs
7. Priority : High
8. Output : Procedure to be followed when Unusual Admin account access is detected

Few General Test cases

1. **Attempts to compromise user credentials [Like Brute Force]**
2. **Unwarranted escalation of privilege**
3. **Misuse of an account**
4. **Unusual behavior on privileged accounts**
5. **Protection against data loss**
6. **System changes**
7. **Instances of Denial of Service**
8. **Detection of malware**
9. **Phishing efforts.**

Monitoring Windows Event Logs

Different types of Logs :

1. Application Log: Event Logged by Application Like Error in starting application is logged
2. System Log : Event Logged By OS Like Failure to start a drive during startup
3. Security Log : event that matters about the security of the system.valid and invalid Logins
4. Directory Service Log: records events of AD. This log is available only on domain controllers.
5. DNS Log: records events for DNS servers and name resolutions. This log is available only for DNS servers

Event types:

1. Information : Event that describes successful completion of task like network drivers loads successfully
2. Warning : Not a threat but should be looked over . Ex Disk space running out
3. Error: Loss of functionality. Like Service fails to load on startup
4. Success Audit (Security Audit) : successful completion of an audited security event.Like user logged in computer
5. Failure Audit (Security Audit) : audited security event that did not complete successfull Like unsuccessful login

Header Information

1. Date The date the event occurred
2. Time The time the event occured
3. User The user who has logged onto the computer when the event occurred
4. Computer The computer where the event occurred
5. Event ID An event number that identifies the event type.

6. Source The source which generated the event. It could be an application or system component Type Type of event (Information, Warning, Error, Success Audit and Failure Audit)