Event viewer

Event Viewer for Incident Response Management

Event Viewer is a powerful tool in Microsoft Windows that allows administrators and security professionals to view logs of system, application, and security events. It is an essential resource for incident response management, helping teams detect, investigate, and mitigate security incidents. Event logs provide a detailed record of activities that can aid in identifying and understanding security events, system issues, and potential breaches.

In the context of incident response management, Event Viewer is often used to monitor, analyze, and respond to security incidents such as unauthorized access, malware infections, system misconfigurations, or potential breaches.

Key Concepts in Incident Response with Event Viewer

Log Sources

Event Viewer categorizes logs into different sources, such as:

- **System**: Logs related to operating system operations.
- **Application**: Logs generated by applications running on the system.
- **Security**: Logs that contain information about security-related events like user logins, access control, and auditing.
- **Setup**: Logs related to the installation and configuration of Windows operating systems and components.
- **Forwarded Events**: Logs forwarded from other machines for centralized logging.

Event Types

Events in the logs can be categorized into several types, which help in identifying the severity and nature of an issue:

- **Information**: Events indicating normal system operations. These are often routine operations.
- **Warning**: Events indicating a potential issue or non-critical event that doesn't stop the system from operating but should be reviewed.
- **Error**: Events indicating significant problems, often related to system or application failures.
- **Critical**: Events representing failures that require immediate attention, usually resulting in a system or service crash.
- **Audit Success/Failure**: Events that track security-relevant activities such as successful/failed logins, object access, privilege use, etc.

Using Event Viewer for Incident Response

Incident response typically follows a series of steps, and Event Viewer plays a critical role in each phase:

1. Preparation

- Set up audit policies to collect necessary security logs (e.g., login attempts, file access, privilege use).
- Ensure proper event log retention and configure log forwarding from endpoints, servers, and devices to centralize logs in a Security Information and Event Management (SIEM) system.

2. Detection

- **Monitoring**: Continuously monitor Security Event Logs for suspicious activities, such as:
  - Unsuccessful login attempts (**Event ID 4625**).
  - Successful logins from unfamiliar or remote locations (**Event ID 4624**).
  - Privilege escalations (e.g., **Event ID 4672** for special privileges).
  - Unexpected or unauthorized service starts/stops (**Event ID 7036**).
  - Changes to critical files or settings.
- **Event Correlation**: Use Event IDs, timestamps, and user information to correlate events across different logs (system, application, security).

3. Analysis

- Investigate the logs by filtering specific Event IDs:
  - **Event ID 4624**: Successful user login (verify user account and source IP).
  - **Event ID 4720**: User account creation (look for unusual accounts being created).
  - **Event ID 4670**: Permissions on an object were changed (could indicate malicious activity).
  - **Event ID 5156**: Windows Filtering Platform (WFP) network traffic events (track potentially malicious traffic).
- **Incident Timeline**: Construct a timeline of events based on the log entries to understand how an attack unfolded.
- **Triage**: Determine the nature and severity of the incident by examining events across multiple sources.

4. Containment

Once a potential breach or security incident is detected, Event Viewer logs can help you:

- Identify the compromised user or machine.
- Confirm unauthorized activities, like remote logins, privilege escalations, or abnormal processes.
- Determine which systems were affected or compromised (e.g., through logs related to malware execution or service crashes).

5. Eradication

Use Event Viewer to locate and eliminate the root cause of the incident:

- Check for malicious software (using logs from antivirus software, services, or system crashes).
- Identify and terminate suspicious processes or services that are running.
- Trace network traffic associated with the compromise using **Event ID 5156 (WFP)**.
- Track user activities that may indicate continued unauthorized access.

6. Recovery

- Restore affected systems from clean backups or system images.
- Verify system integrity and application functionality by reviewing logs to ensure no residual malicious activity remains.
- Monitor systems closely after recovery for signs of recurring incidents.

Commonly Used Event IDs for Incident Response

Here are some key Event IDs relevant to incident response:

- **Event ID 4624**: Successful logon (indicates a successful user login).
- **Event ID 4625**: Failed logon (indicates a failed login attempt).
- **Event ID 4768**: Kerberos authentication ticket request (used in attacks like Pass-the-Ticket).
- **Event ID 4672**: Special privileges assigned to a new logon (e.g., admin privileges).
- **Event ID 4720**: User account creation (may indicate a malicious actor creating accounts).
- **Event ID 4740**: Account locked out (indicates brute-force attempts).
- **Event ID 4634**: Logoff event (records when a user logs off).
- **Event ID 5156**: Windows Filtering Platform (WFP) network traffic events (useful for monitoring network traffic).
- **Event ID 4688**: New process creation (helps detect suspicious executables or malware).
- **Event ID 7036**: Service state change (may indicate unauthorized service manipulation).
- **Event ID 1102**: Audit log cleared (may indicate tampering to cover tracks).

Best Practices for Event Viewer in Incident Response

- **Enable Advanced Auditing**: Configure Windows to record detailed security events, such as logon attempts, account modifications, group membership changes, and file access.
- **Log Retention and Archiving**: Ensure logs are retained for a sufficient period for compliance and forensic investigations. Use a SIEM system to aggregate and analyze logs from multiple machines.
- **Centralized Logging**: For large organizations, configure centralized logging for all critical systems using tools like Windows Event Forwarding (WEF) or SIEM systems.
- **Regular Log Reviews**: Periodically review event logs to identify anomalous activities before they escalate into incidents.
- **Use Filtering and Alerts**: Set up filters and automated alerts for critical events (e.g., multiple failed logons attempts or privilege escalations) to respond in real time.
- **Incident Playbooks**: Develop standardized incident response playbooks that outline steps to follow when specific suspicious activities are detected via Event Viewer logs.
- **Security Baselines**: Establish a baseline of normal system activity using Event Viewer data to more easily detect anomalies and unusual behaviours.