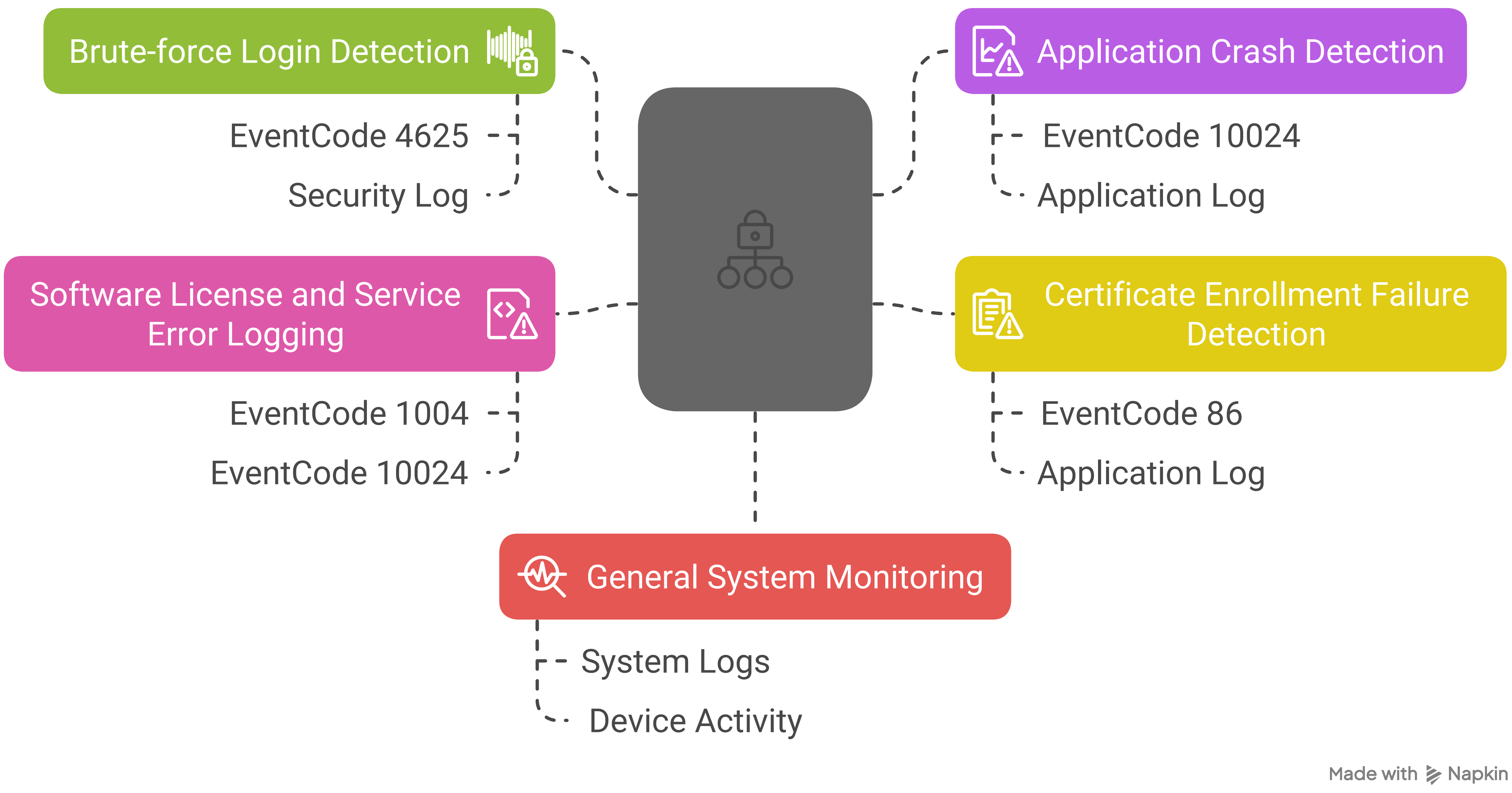
Splunk Threat Detection Project Report

This document outlines the steps taken in a project that utilizes Splunk for monitoring and analyzing Windows Event Logs to identify common attack patterns and system events. The report details the objectives, use cases implemented, tools and environment used, SPL queries executed, and concludes with the effectiveness of Splunk in real-time log analysis and threat detection.

1. Objective

This project uses Splunk to monitor and analyze Windows Event Logs to detect common attack patterns and system events.

2. Use Cases Implemented



Brute-force Login Detection
EventCode 4625
Security Log
Application Crash Detection
EventCode 10024
Application Log
Software License and Service Error Logging
EventCode 1004
EventCode 10024
Certificate Enrollment Failure Detection
EventCode 86
Application Log
General System Monitoring
System Logs
Device Activity
Made with Napkin

3. Tools & Environment

- **Splunk Enterprise** installed on Windows 10
- **Log Sources**:
    - WinEventLog:Security
    - WinEventLog:Application
    - WinEventLog:System

4. SPL Queries Used

brute_force_logins.spl:

```
index=main OR index=default sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, Workstation_Name
| where count > 5
```

application_crashes.spl:

```
index=main sourcetype=WinEventLog:Application
| search Message="forcibly terminated"
| table _time, Source, EventCode, Message
```

system_device_activity.spl:

```
index=main sourcetype=WinEventLog:System
| table _time, Source, EventCode, Message
```

# Note: No system-related results were observed in this session.

5. Conclusion

This project demonstrates how Splunk can be effectively used for real-time log analysis and threat detection across multiple Windows log sources.Although system logs returned no data in this instance, the workflow lays the foundation for ongoing monitoring and SIEM development. It serves as a strong foundation for building a home-based SIEM system.