**Cyber Forensics and Threat Detection Dashboard**

**Abstract**

Cyber threats are an evolving challenge in modern digital infrastructures, requiring continuous monitoring and forensic analysis for effective incident response. This project introduces a Cyber Forensics and Threat Detection Dashboard, a system designed to analyze event logs, detect suspicious activities, and compute a risk score based on detected anomalies. The tool integrates cybersecurity principles with digital forensics methodologies, enabling proactive threat detection and forensic investigation. This paper details the system's architecture, key functionalities, implementation, evaluation, and future enhancements.

**Introduction**

The rise in cyber threats, including unauthorized access, malware infections, and system breaches, has necessitated the development of forensic tools for rapid incident analysis. Traditional Security Information and Event Management (SIEM) systems provide log aggregation but lack comprehensive forensic capabilities. The proposed system combines forensic log analysis with real-time threat detection, assigning risk scores based on observed security incidents. This system is designed to assist cybersecurity professionals in incident response and digital forensics investigations.

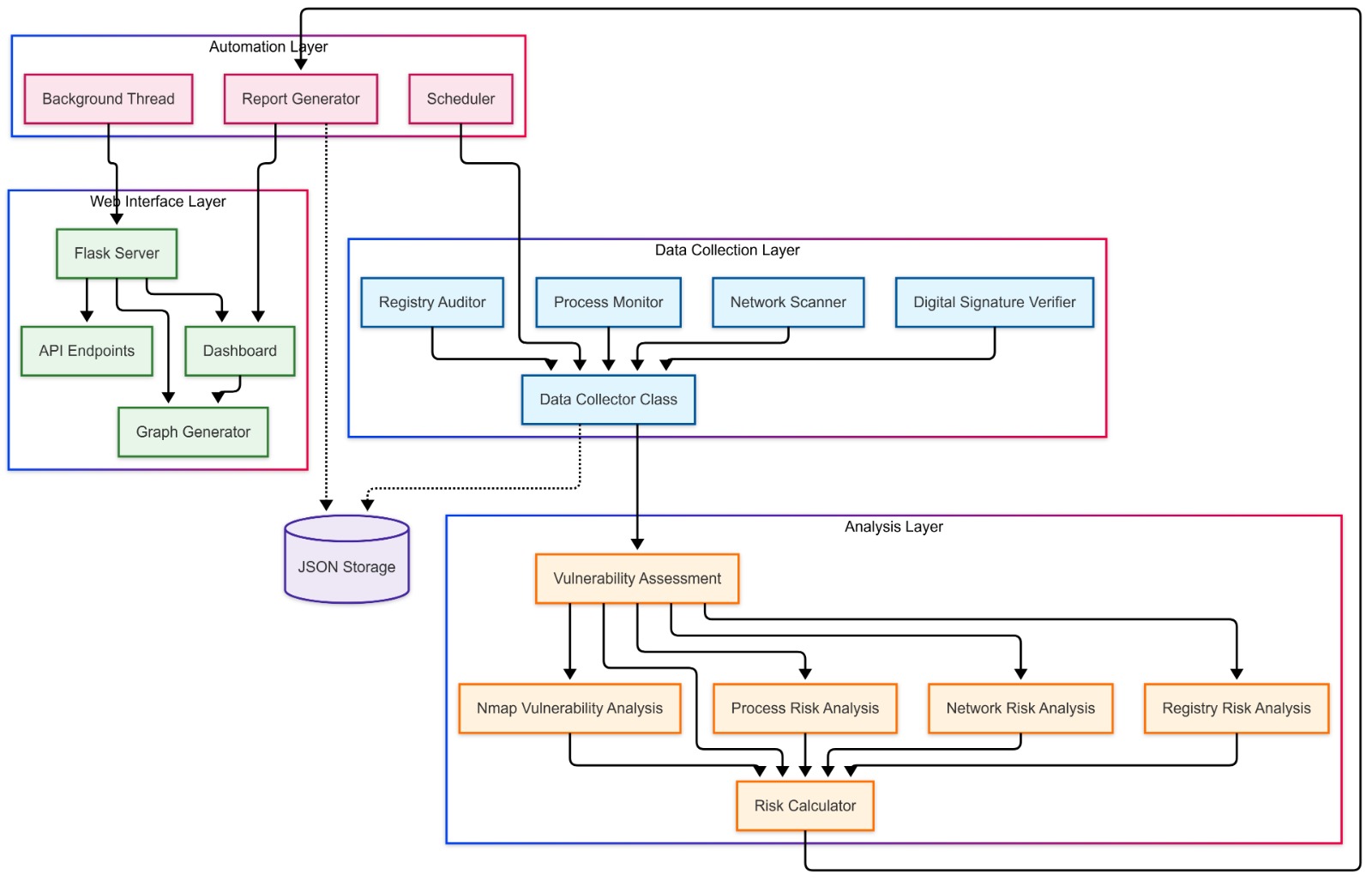
**Objectives**

* **Cyber Forensics:** Capture and analyse system logs (Windows Event Logs and Linux Syslogs) for forensic investigations.
* **Threat Detection:** Identify and flag suspicious activities, including failed logins, unauthorized process executions, and network anomalies.
* **Risk Assessment:** Compute dynamic risk scores based on security events, providing a quantified risk posture.
* **Incident Response:** Support forensic investigations by preserving logs, generating reports, and maintaining a chain of custody to ensure evidence integrity.

**System Architecture**

The proposed system consists of three core layers:

1. **Data Collection Layer:** Acquires system logs, process details, and network activity from multiple sources.
2. **Threat Analysis Engine:** Processes collected data, applies forensic rules, and calculates risk scores based on predefined indicators.
3. **Visualization & Reporting Layer:** Presents forensic findings through a dashboard with historical risk trend analysis and detailed logs for further investigation.



**Methodology**

**Event Log Analysis**

* **Windows:** Extracts and analyzes Security, System, and Application logs using Windows Event Log APIs.
* **Linux:** Retrieves and processes Syslog files (/var/log/auth.log, /var/log/syslog) for login attempts and system modifications.
* **Forensic Significance:** Identifies key security events such as failed login attempts (Event ID 4625), audit log clearance (1102), and process executions (4688), which are crucial in tracking unauthorized access attempts and system modifications.

**Evidence Collection**

* Generates and stores forensic snapshots of running processes, network connections, and registry modifications.
* Computes cryptographic hash values (SHA256) to ensure the integrity and authenticity of collected artifacts.
* Logs user interactions and system changes to maintain forensic integrity and support legal compliance for court-admissible evidence.

**Threat Detection Components**

**Process and Network Monitoring**

* Identifies unauthorized running processes, potential malware signatures, and abnormal network activity.
* Flags unusual open ports and high-port utilization, which could indicate unauthorized access attempts or malware command-and-control operations.

**Registry Analysis (Windows)**

* Extracts startup entries and detects unrecognized applications that may be linked to persistence mechanisms used by malware.
* Monitors unauthorized registry modifications that indicate potential system compromise or privilege escalation attempts.

**Nmap-Based Vulnerability Scanning**

* Identifies exposed services using Nmap scanning to detect open ports and active network services.
* Maps detected services to known vulnerabilities using publicly available exploit databases, aiding forensic investigations by identifying potential attack vectors.

**Risk Scoring Model**

The system computes a risk score based on weighted security events, enabling analysts to prioritize investigations.

|  |  |  |
| --- | --- | --- |
| Security Event | Example Identifiers | Assigned Risk Points |
| Failed Logins | 4625 (Windows), 'Failed password' (Linux) | +2 per event |
| Audit Log Cleared | 1102 (Windows) | +5 per event |
| Process Execution | 4688 (Windows) | +2 per event |
| Unauthorized Registry Modification | Registry Key Tampering | +3 per event |
| Open High Ports | Detected via Nmap | +3 per event |

**Implementation**

* **Programming Languages:** Python (backend), HTML/CSS, JavaScript (frontend).
* **Frameworks & Libraries:** Flask (API & UI), Bootstrap (visualization), Matplotlib (risk trend analysis), Win32 API (Windows logs), OS/System modules (Linux logs).
* **Data Storage:** JSON-based storage for log data and risk assessment records, ensuring efficient retrieval and forensic reporting.

**Evaluation & Testing**

* Conducted controlled experiments to validate event log analysis accuracy and system performance.
* Simulated real-world attack scenarios to assess the effectiveness of forensic evidence collection.
* Verified forensic data integrity using cryptographic hash validation to prevent data tampering.
* Compared results with known forensic frameworks to ensure accuracy and completeness of findings.

**Future Enhancements**

* **Integration with SIEM Solutions:** Compatibility with Splunk, ELK Stack to enhance log aggregation and real-time threat intelligence.
* **Automated Report Generation:** Export forensic findings to PDF/CSV formats for legal and investigative use.
* **Memory Forensics Integration:** Support for the Volatility framework to analyze memory dumps and detect hidden threats in volatile memory.
* **Machine Learning-Based Anomaly Detection:** Implement AI-driven analysis to detect zero-day threats and insider attacks.

**Conclusion**

The Cyber Forensics and Threat Detection Dashboard enhances system security monitoring by integrating forensic analysis with risk-based threat detection. The system provides real-time event log monitoring, evidence collection, and risk assessment, supporting incident response and forensic investigations. By combining cybersecurity methodologies with forensic best practices, this tool offers a robust solution for detecting and analyzing cyber threats. Future improvements include automated reporting, memory forensics, and deeper integration with threat intelligence platforms, making it a scalable forensic investigation framework.

**References**

* NIST Cybersecurity Framework
* MITRE ATT&CK Framework
* Windows Event Logging Documentation
* Linux Syslog Documentation
* Digital Forensics Incident Response Best Practices