1. **Network Traffic Monitoring**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Sub-category** | **Metric / Format** | |  |  | | --- | --- | |  | **Frequency** | | **Collection Mode** | **Collection Mechanism** | **Recorded At** | **Storage** |
| Network | |  |  | | --- | --- | |  | Protocol | | Text | Real-time | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | |  | Network Tap | | Gateway Router | CSV File |
| Network | Throughput | |  |  | | --- | --- | |  | Numeric (Mbps) | | Real-time | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | |  | NetFlow / sFlow | | Core Switch | CSV File |
| Network | |  |  | | --- | --- | |  | Source IP | | |  |  | | --- | --- | |  | Text | | Real-time | |  |  | | --- | --- | | Automated |  | | Packet Capture (PCAP) | Firewall | Log File |
| Network | Destination Port | Numeric | Real-time | |  |  | | --- | --- | | Automated |  | | Deep Packet Inspection | Gateway Router | Database Table |
| Network | Bandwidth Usage | Numeric (MB/hr) | Hourly | |  |  | | --- | --- | | Automated |  | | SNMP | Network Interface | Excel File |

1. **Endpoint Monitoring**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Sub-category** | **Metric / Format** | |  |  | | --- | --- | |  | **Frequency** | | **Collection Mode** | **Collection Mechanism** | **Recorded At** | **Storage** |
| Endpoint | Operating System Version   |  |  | | --- | --- | |  |  | | Text | Daily | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | |  | WMI / PowerShell | | Host Machines | CSV File |
| Endpoint | Firewall Status | |  |  | | --- | --- | |  | Boolean | | Daily | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | |  | PowerShell Script | | Host Machines | CSV File |
| Endpoint | |  |  | | --- | --- | | Antivirus Signature Updated |  | | |  |  | | --- | --- | |  | Boolean | | Daily | |  |  | | --- | --- | | Automated |  | | AV Logs | Host Machines | Excel File |
| Endpoint | Disk Usage | Numeric (GB) | Hourly | |  |  | | --- | --- | | Automated |  | | WMI Monitoring | Host Machines | Database Table |
| Endpoint | CPU Usage | Numeric (%) | Real-time | |  |  | | --- | --- | | Automated |  | | Performance Monitor | Host Machines | CSV File |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Sub-category** | **Metric / Format** | |  |  | | --- | --- | |  |  |   **Frequency** | **Collection Mode** | **Collection Mechanism** | **Recorded At** | **Storage** |
| Backup | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  | Coverage | |  | | Percentage | Daily | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | | Backup Tool Logs |  | | Backup Server | |  | | --- | | Excel File | |
| Backup | |  | | --- | | Encryption Status | | |  |  | | --- | --- | |  | Boolean | | Daily | |  |  | | --- | --- | | Automated |  | | |  |  | | --- | --- | |  | Backup Config Reports | | Backup Server | CSV File |
| Backup | |  |  | | --- | --- | | Validation Status |  | | |  |  | | --- | --- | |  | Text (Pass/Fail) | | Daily | |  |  | | --- | --- | | Automated |  | | |  | | --- | | Backup Validation Logs | | Backup Server | CSV File |
| Backup | |  | | --- | | Last Backup Timestamp | | |  | | --- | | Timestamp | | Daily | |  |  | | --- | --- | | Automated |  | | |  | | --- | | Job Scheduler Logs | | Backup Server | |  | | --- | | Log File | |
| Backup | |  | | --- | | Storage Location | | Text | Weekly | |  |  | | --- | --- | | Manual |  | | |  | | --- | | Backup Admin Entry | | Admin Terminal | |  | | --- | | Excel File | |

1. **Data Backup Monitoring**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Sub-category** | **Metric / Format** | |  |  | | --- | --- | |  |  |   **Frequency** | **Collection Mode** | **Collection Mechanism** | **Recorded At** | **Storage** |
| Staff | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | | Training Completed |  | |  | | |  |  | | --- | --- | |  | Boolean | | Quarterly | Manual | |  |  | | --- | --- | | HR Records |  | | HR System | |  | | --- | | Excel File | |
| Staff | |  | | --- | | Current Risk Profile | | |  |  | | --- | --- | |  | 3-Scale (Low/Med/High) | | Quarterly | Manual | |  |  | | --- | --- | |  | Cyber Awareness Survey | | HR System | CSV File |
| Staff | |  |  | | --- | --- | | Pending Training |  | | |  |  |  |  | | --- | --- | --- | --- | |  |  | Boolean | T | | Monthly | Manual | |  | | --- | | LMS Report | | HR System | Excel File |
| Staff | |  | | --- | | Role Risk Profile | | |  | | --- | | 5-Scale | | Quarterly | Manual | |  | | --- | | Role-Based Mapping | | HR System | |  | | --- | | CSV File | |
| Staff | |  | | --- | | Phishing Simulation Results | | Numeric (%) | Monthly | |  |  | | --- | --- | | Automated |  | | |  | | --- | | Simulation Platform | | Email System | |  | | --- | | Excel File | |

1. **Staff Readiness Monitoring**

**Important Factors in Data Collection for Cybersecurity Monitoring**

*The data collection model and processes provided in the table above are crucial for establishing a robust monitoring system. Based on the data structure mentioned above, the following key factors have been identified to ensure the successful monitoring of network traffic, endpoints, data backups, and staff readiness. These elements play a pivotal role in enhancing cybersecurity defences and should be taken into account for effective monitoring.*

**1. Network Traffic Monitoring:**

* **Protocol**: As per the data structure mentioned above, monitoring protocols in real-time allows for quick identification of malicious or unauthorized network traffic.
* **Throughput**: By tracking throughput, network performance can be assessed, with anomalies suggesting potential DDoS attacks or data exfiltration, as highlighted in the data collection strategy.
* **Source IP & Destination Port**: The data structure specifies the need to track source IP and destination ports in real-time, as unusual activity can indicate potential threats or unauthorized access attempts.
* **Bandwidth Usage**: Regular monitoring of bandwidth usage, as noted in the data collection plan, helps identify sudden increases or decreases in traffic, which could point to security breaches or other malicious activity.

**2. Endpoint Monitoring:**

* **Operating System Version**: The table above suggests monitoring OS versions regularly to ensure that all endpoints are up-to-date with the latest security patches and fixes.
* **Firewall Status**: The data structure emphasizes monitoring firewall status on endpoints to ensure they are active and functional to defend against attacks.
* **Antivirus Signature Updates**: As specified in the table, keeping antivirus signatures updated is essential for protecting endpoints against the latest malware threats.
* **Disk Usage**: Monitoring disk usage helps detect unusual activity on endpoints, such as file modifications related to ransomware, as indicated in the data collection strategy.
* **CPU Usage**: Real-time monitoring of CPU usage, as shown in the table, can identify processes consuming abnormal CPU power, which could be a sign of malware activity.

**3. Data Backup Monitoring:**

* **Backup Coverage**: The data structure advises tracking the percentage of critical data covered by backups to ensure that vital data is protected and can be restored when needed.
* **Backup Encryption Status**: Ensuring backups are encrypted, as suggested in the table, protects sensitive data in case of theft or unauthorized access.
* **Backup Validation Status**: Regular validation of backups, as noted in the data structure, ensures they are functional and can be used for recovery in case of data loss or corruption.
* **Last Backup Timestamp**: Keeping track of the last backup timestamp, as mentioned in the table, ensures that backups are current and minimizes data loss during a recovery process.
* **Storage Location**: The data collection model suggests monitoring backup storage locations to ensure their security and availability for recovery purposes.

**4. Staff Readiness Monitoring:**

* **Training Completed**: The table suggests tracking training completion to ensure staff are equipped to handle cyber threats and reduce the risk of human error.
* **Current Risk Profile**: Understanding staff risk profiles, as per the data structure, helps prioritize security efforts based on departmental or role-specific vulnerabilities.
* **Pending Training**: Identifying pending training, as indicated in the table, ensures that all employees receive the necessary cybersecurity training to stay informed about emerging threats.
* **Phishing Simulation Results**: Regular phishing simulations, as outlined in the data collection model, assess staff preparedness and help improve their ability to identify phishing attempts.
* **Role Risk Profile**: The table recommends tracking role-based risk profiles to identify high-risk staff and tailor security measures accordingly.

*In conclusion, the data collection model outlined above provides a structured approach to monitor network traffic, endpoints, backups, and staff readiness. By leveraging real-time and automated collection methods, the government organization can proactively detect threats, ensure data protection, and improve staff preparedness. This model will strengthen overall cybersecurity defences and help mitigate the risk of malware attacks.*