Data

1. Indicators of Compromise (IoCs)

- **Malicious IP Addresses**: Track known or suspected malicious IPs to detect communication with threat actors.
- **Malicious URLs and Domains**: Monitor URLs or domains associated with phishing sites, malware, or other malicious activities.
- **File Hashes**: Gather hashes (MD5, SHA1, SHA256) of known malicious files to detect malware on your network.
- **Email Addresses**: Look for email addresses used in phishing attempts or other social engineering tactics.

2. Network Traffic Data

- **Connection Logs**: Capture logs of inbound and outbound network traffic, including source and destination IPs, ports, and protocols.
- **Unusual Traffic Patterns**: Identify traffic anomalies such as high volumes of data transfer, connections to unfamiliar geographic regions, or irregular communication patterns.
- **Network Intrusion Detection System (NIDS) Alerts**: Use NIDS to detect suspicious activity on the network.

3. User Activity and Behavior Data

- **Login and Authentication Logs**: Collect logs of successful and failed login attempts, including time, location, and device details.
- **User Account Changes**: Monitor account creation, privilege escalation, or other changes to user accounts that may indicate a threat.
- **Behavioral Anomalies**: Detect deviations from typical user behavior, such as accessing data outside of regular hours or unusual download activity.

4. Endpoint Security Data

- **Antivirus and Anti-malware Alerts**: Record alerts from endpoint security software that indicate potential threats like detected malware or suspicious behavior.
- **File Changes and Integrity Monitoring**: Detect changes to critical system files that could indicate a breach or malware infection.
- **Installed Software Logs**: Track newly installed or modified software, especially if it runs unexpectedly.

5. System and Server Logs

- **Application Logs**: Monitor logs from critical applications to detect unauthorized access, failed logins, or abnormal error messages.
- **Operating System Logs**: Collect logs from system events, such as unusual reboots, services starting/stopping unexpectedly, or system configuration changes.
- **Web Server Logs**: Review web server access logs for suspicious requests, SQL injection attempts, or excessive requests from a single IP address.

6. Email Security Data

- **Spam and Phishing Detection Logs**: Monitor spam filter logs to identify potentially harmful emails.
- **Suspicious Email Attachments or Links**: Collect information on attachments or embedded links in emails that may contain malicious content.

7. Threat Intelligence Feeds

- **Threat Actor Information**: Gather data about known threat actors, including their tactics, techniques, and procedures (TTPs).
- **Real-time Threat Feeds**: Integrate feeds that provide information about newly discovered threats, zero-day exploits, or other emerging risks.
- **Reputation Scores**: Use data enrichment services to get reputation scores for IP addresses, domains, or file hashes.

8. Vulnerability Data

- **Open Ports and Services**: Monitor network services and open ports for signs of unnecessary exposure.
- **Patch Management Data**: Keep track of which systems are up to date with security patches and which are vulnerable.
- **Configuration Vulnerabilities**: Identify misconfigured security settings that could be exploited by attackers.

9. Incident Response Data

- **Incident Reports and Alerts**: Collect details of any security incidents or alerts, including the source, type of threat, and time of occurrence.
- **Mitigation Actions Taken**: Document the steps taken to mitigate threats, including patching, blocking, or quarantining.
- **Forensic Data**: Store digital forensic evidence, such as memory dumps or disk images, for further analysis.

10. Physical Security Logs

- **Access Control Systems**: Monitor physical access logs for unusual activity at data centers or other sensitive areas.
- **Camera Surveillance**: Record footage and analyze for suspicious activity around critical infrastructure.

11. Cloud and Virtual Environment Data

- **Cloud Activity Logs**: Collect logs from cloud services (AWS, Azure, Google Cloud) for unusual activity like unexpected API calls or data transfers.
- **Virtual Machine Monitoring**: Keep track of VM creation, deletion, and changes that might indicate a threat.