UNIVERSIDADE BEIRA INTERIOR

SNAKEY

1. IDENTIFY (Asset Management, Risk Assessment)

Goal: Establish a baseline of user behavior and define security policies.

Key Features & Implementation:

- **User Role & Context Awareness:**
  - Maintain a mapping of users to their roles (e.g., Admins, Standard Users). This helps in assigning appropriate access rights and monitoring behaviors based on roles.
  - Store baseline behaviors for each user, such as normal login times and typing habits. This helps detect anomalies if a user behaves differently from their established pattern.
- **Threat Intelligence Integration:**
  - Integrate with external threat intelligence platforms like AbuseIPDB, VirusTotal API, and AlienVault OTX to identify known malicious IPs.
  - Automatically update blocklists based on the latest threat feeds and perform geolocation lookups to verify the legitimacy of user logins from various locations.
- **Baseline User Behavior (Behavioral Profiling):**
  - Use machine learning to analyze user typing patterns (speed, pauses, errors) and track typical command sequences.
  - Store these behavior profiles in a database (SQLite for local storage or cloud-based for scalability), enabling comparison of current behavior with the baseline to detect anomalies.
- **Tracking Privileged Access & Anomalies:**

    - Flag unauthorized access attempts to sensitive files or directories.
    - Monitor commands like `net user /add` or `whoami /priv` that indicate potential privilege escalation attempts and alert security teams when detected.

---

2. PROTECT (Access Control, Data Security, Safeguards)

Goal: Ensure the security and integrity of collected data while protecting user privacy.

Key Features & Implementation:

- **Encryption & Secure Storage:**
    - Use AES-256 encryption for data security, combined with CRYSTALS-Kyber/ ASCON key exchange for secure key generation during each session.
    - Encrypt logs in real-time using AES-GCM, ensuring data integrity and authenticity.
    - Store encrypted logs in an append-only database (MongoDB for large-scale storage or SQLite for smaller deployments).
- **Stealth & Integrity Protection:**
    - Implement hidden installation methods, such as stealth services on Windows, to avoid detection by attackers.
    - Include anti-tampering mechanisms like periodic hash checks of the executable to verify its integrity, and a watchdog process to self-repair if the program is modified or deleted.
- **Preventative Monitoring for Unauthorized Activities:**
    - Block the execution of high-risk tools like `cmd.exe`, `PowerShell`, and `net user` unless explicitly whitelisted.
    - Monitor registry edits, especially changes to startup programs that might indicate malware persistence mechanisms.
    - Alert security teams when USB mass storage devices are inserted, reducing the risk of data exfiltration.
- **Compliance & Privacy Controls:**
    - Ensure logs are encrypted both at rest and during transmission.
    - Implement Role-Based Access Control (RBAC) to restrict log access based on user roles.
    - Ensure all operations comply with the **Código de Integridade da Universidade da Beira Interior** to maintain data privacy and integrity.

---

3. DETECT (Threat Detection, Anomaly Detection, Behavioral Analytics)

Goal: Identify insider threats, brute-force attempts, and unusual system behavior.

Key Features & Implementation:

- **Keystroke Behavior Analysis:**
  - Detect potential automation by flagging excessive typing speeds (e.g., >150 WPM).
  - Monitor for rapid and repeated failed login attempts, a strong indicator of brute-force attacks.
- **Command Execution Monitoring:**
  - Track the execution of high-risk commands like `whoami`, `wmic process`, and `net user`.
  - Use regex to detect suspicious PowerShell scripts, including base64 encoded commands that might be used by attackers to obfuscate their actions.
- **Anomaly-Based Contextual Alerts:**
  - Detect off-hours access attempts, such as user logins during unusual times (e.g., 2 AM).
  - Flag logins from unexpected locations (e.g., foreign countries), which might indicate compromised credentials.
- **Threat Scoring System:**
  - Assign dynamic risk scores based on observed behavior:
    - Suspicious command execution: +7 points
    - High typing speed: +3 points
    - Unknown application execution: +5 points
  - Trigger alerts when the total risk score reaches or exceeds 10 points.
- **Live Monitoring Dashboard (Real-Time Alerts & Reports):**
  - Display heatmaps of typing activity across different times of the day.
  - Provide visualizations of flagged commands and other suspicious activities.
  - Integrate with Slack API to send real-time notifications to the Security Operations Center (SOC) team.

---

4. RESPOND (Incident Response, Alerting & Automated Actions)

Goal: Implement automated threat mitigation and escalation workflows.

Key Features & Implementation:

- **Automated Escalation Path:**
  - **1st Level (Warning):** Log the event and notify the user of the suspicious activity.
  - **2nd Level (SOC Alert):** Send an alert to the security team if the risk score is ≥10.
  - **3rd Level (Quarantine):** Automatically lock the user session in case of extreme behavior anomalies.
- **Dynamic Trust Levels & Adaptive Authentication:**
  - Require additional authentication, such as Time-based One-Time Passwords (TOTP), when suspicious behavior is detected.
  - Implement session-generated credentials for flagged sessions to add another layer of security.
- **Threat Intelligence Updates & Automated Countermeasures:**
  - Dynamically block users' IP addresses if they are linked to known threats.
  - Disable account access if multiple high-risk activities occur in a short time frame.
- **Automated Threat Response via API Hooks:**
  - Capture screenshots when suspicious commands are executed, aiding forensic investigations.
  - Collect metadata of active windows during flagged activities.
  - Automatically trigger SOC notifications and screenshots if a flagged IP is detected.

---

5. RECOVER (Post-Incident Analysis, Learning & Refinement)

Goal: Improve security resilience and refine threat detection over time.

Key Features & Implementation:

- **Log Review & Forensics:**
  - Store encrypted keystroke logs to allow post-incident analysis.
  - Generate comprehensive security reports for review by the SOC team.
- **Adaptive Whitelisting & False Positive Reduction:**
  - Allow the security team to add flagged behaviors to the whitelist if verified as safe.
  - Implement context-aware whitelisting (e.g., security admins can run `net user` commands without triggering alerts).
- **Machine Learning for Continuous Improvement:**
  - Continuously compare current user behavior against historical trends.
  - Retrain detection models periodically to adapt to new behavior patterns and threats.
- **Purple Teaming & Penetration Testing:**
  - Conduct simulated attacks to test the effectiveness of the security system.
  - Organize SOC drills using red team tactics to enhance the system's readiness against advanced threats.
- **Incident Response Drills & Playbooks:**
  - Develop and maintain incident response playbooks for handling different types of security incidents.
  - Regularly train security teams on detecting and mitigating threats using the system, ensuring a rapid and effective response during real incidents.

Access Control (PR.AC-1, PR.AC-3)	Uses Role-Based Access Control (RBAC) to manage user permissions and ensure only authorized users access logs.
Encryption (PR.DS-1, PR.DS-2, PR.DS-3)	Uses AES-256 and CRYSTALS-Kyber/Ascon for encrypting keystroke logs in storage and transmission.
Integrity Protection (SI-7, AU-10)	Hash checks for executable integrity, ensuring Sneaky is not modified or tampered with.
Anomaly Detection (DE.AE-2, AU-6, CA-7)	Behavioral profiling via ML to detect deviations in user activity, flagging suspicious behaviors.

Incident Response (RS.AN-1, RS.CO-2)	Automatically alerts security teams when anomalies exceed a predefined risk score.
Logging & Audit Trails (AU-3, AU-12, AU-14)	Stores encrypted logs in an append-only database to maintain audit integrity.
Privacy & Compliance (PT-2, PT-3, PT-7)	Ensures logs are encrypted and role-based access is enforced to protect sensitive data.

Internal Audit – Perform a self-assessment against **NIST 800-53 or CSF**.