📌 **Objective:**  
Develop an **AI-driven security solution** that automates **vulnerability assessments, compliance checks, log analysis, and risk evaluation** for an IT organization. The project will use **machine learning (ML) models** to detect threats, predict security risks, and ensure compliance with industry standards (ISO 27001, NIST, GDPR).

**1️⃣ Project Scope & Key Areas**

|  |  |  |
| --- | --- | --- |
| **Security Area** | **AI-Driven Solution** | **Security Risk Addressed** |
| **Vulnerability Assessment** | Automated scanning & risk classification using AI | Identify & rank security flaws |
| **Compliance Checks** | NLP-based policy enforcement & audit automation | Ensure regulatory compliance |
| **Log Analysis & SIEM** | AI-based anomaly detection in logs | Detect suspicious activity |
| **Risk Evaluation** | Predictive analytics for cyber risk scoring | Prioritize security threats |

**2️⃣ Project Team & Roles**

👨‍💻 **Student 1: AI & Machine Learning Engineer**  
✅ Develops **ML models** for log analysis & anomaly detection  
✅ Uses **TensorFlow, PyTorch, and Scikit-learn**  
✅ Implements **threat classification & predictive security scoring**

👨‍💻 **Student 2: Cybersecurity & Compliance Expert**  
✅ Conducts **vulnerability scans & compliance checks**  
✅ Uses **Nmap, OpenVAS, and CIS Benchmarks**  
✅ Ensures security policies align with **ISO 27001, NIST, GDPR**

👨‍💻 **Student 3: Software & Automation Developer**  
✅ Develops **security automation scripts** in Python  
✅ Implements **AI-powered SIEM & log monitoring**  
✅ Uses **ELK Stack, Splunk, and Security Onion**

**3️⃣ Tools & Technologies for Implementation**

|  |  |  |
| --- | --- | --- |
| **Category** | **Tool/Technology** | **Usage** |
| **AI/ML** | TensorFlow, PyTorch | Anomaly detection, risk scoring |
| **Vulnerability Scanning** | OpenVAS, Nmap | Identify security weaknesses |
| **Compliance Auditing** | CIS Benchmarks, NIST Security Controls | Verify security compliance |
| **Log Analysis & SIEM** | ELK Stack, Splunk, Security Onion | Log monitoring & alerting |
| **Threat Intelligence** | MITRE ATT&CK, VirusTotal API | Identify known attack patterns |
| **Automation & Scripting** | Python, Bash, PowerShell | Automate security checks |

**4️⃣ Implementation Steps**

**📌 Phase 1: Research & Threat Modeling (Weeks 1-2)**

✅ Study **common vulnerabilities & risk assessment frameworks**  
✅ Identify compliance requirements (**ISO 27001, NIST, GDPR**)  
✅ Define AI model objectives (log analysis, anomaly detection, risk prediction)

**📌 Phase 2: AI Model Development (Weeks 3-6)**

🛠️ **1. AI for Log Analysis & Anomaly Detection**  
✅ Collect logs from **firewalls, IDS/IPS, and authentication systems**  
✅ Train an **unsupervised ML model** (e.g., Autoencoder, Isolation Forest) for anomaly detection  
✅ Classify security events using **CNNs or LSTMs**

🛠️ **2. Automated Vulnerability Assessment**  
✅ Integrate **OpenVAS & Nmap** for network vulnerability scanning  
✅ Use **AI-based risk scoring** to prioritize vulnerabilities

🛠️ **3. Compliance Automation**  
✅ Develop **policy enforcement scripts** to detect misconfigurations  
✅ Automate compliance audits using **NIST & CIS Benchmarks**

**📌 Phase 3: Security Dashboard & Automation (Weeks 7-9)**

✅ Develop a **real-time monitoring dashboard** using ELK Stack/Splunk  
✅ Integrate AI models for **risk prediction & alerting**  
✅ Automate **incident response workflows**

**📌 Phase 4: Testing & Deployment (Weeks 10-12)**

✅ Test AI model accuracy on **real-world security datasets**  
✅ Simulate **cyberattacks** to validate anomaly detection effectiveness  
✅ Document findings & submit **final report & research paper**

**5️⃣ Expected Outcomes & Deliverables**

✅ **AI-driven vulnerability scanner & risk assessment tool**  
✅ **Compliance automation scripts** for security audits  
✅ **SIEM-powered log analysis system** with anomaly detection  
✅ **Final research paper on AI-driven cybersecurity automation**