Bekhzod Anvarov

Cybersecurity Analyst

Rilevamento delle intrusioni di rete, analisi del traffico di rete, rilevamento delle anomalie

Torino, Italia
virtsudo@proton.me | virtsudo.me | linkedin.com/in/virtsudo | github.com/virtsudo

PROFILO

Laurea magistrale in Ingegneria Informatica (percorso Cybersecurity) al Politecnico di Torino, con focus sul rilevamento delle intrusioni di rete. Nella tesi ho sviluppato e testato una pipeline di rilevamento delle intrusioni su traffico reale di backbone degli anni 2011, 2016 e 2021. Disponibile per posizioni junior e tirocini nella cybersecurity, in presenza o da remoto.

FORMAZIONE

Laurea Magistrale in Ingegneria Informatica (Computer Engineering), percorso Cybersecurity
Politecnico di Torino, 2026

Laurea Triennale in Ingegneria Informatica
Politecnico di Torino, 2022

ESPERIENZA DI RICERCA

JEPA Representation Learning for Intrusion Detection on Real-World Drifting Network Traffic
Tesi di laurea magistrale, Politecnico di Torino, 2026
Relatori: Prof. Guido Marchetto, Prof. Alessio Sacco, Dott. Cristiano Serra
Una rappresentazione appresa da traffico di rete non etichettato permette a un classificatore di intrusioni di restare più accurato che con le feature di flusso grezze su traffico registrato anni dopo?

- **Sviluppo** in Python di una pipeline di rilevamento delle intrusioni con preprocessing dei flussi, un modello JEPA self-supervised in PyTorch e quattro classificatori (regressione logistica, albero decisionale, random forest, XGBoost), su traffico reale di backbone degli anni 2011, 2016 e 2021 (benchmark MAWIFlow, feature CICFlowMeter, etichette MAWILab).
- **Test** dei classificatori di ogni anno su tutti gli anni. La rappresentazione ha reso le anomalie più separabili linearmente, ma non ha ridotto il calo tra gli anni, e dopo il 2011 le etichette hanno cambiato significato.
- **Verifica** del benchmark. Ho sostituito la sua normalizzazione, che faceva perdere gran parte della risoluzione delle feature, e ho rilevato che le metriche pubblicate contraddicono i campioni pubblicati per due dei tre anni.

Tecnologie: Python, PyTorch (CUDA), scikit-learn, XGBoost, Polars, NumPy, Matplotlib

PROGETTI

Laboratori di Deep Learning per la Cybersecurity
Tecnologie: Python, PyTorch, Jupyter, Hugging Face
Sviluppo di una FFNN per il rilevamento delle intrusioni di rete e di modelli FFNN, RNN e GNN per classificare malware. Fine-tuning di BERT per analizzare log SSH ed etichettarli con le tattiche MITRE ATT&CK.
GitHub: github.com/virtsudo/dl-cybersecurity-labs

COMPETENZE

Strumenti di sicurezza (corsi universitari): Wireshark, Nmap, Burp Suite
Programmazione e strumenti: Python, C/C++, SQL (MySQL, SQLite), shell Linux, Git/GitLab
Machine learning: PyTorch, scikit-learn, XGBoost, Hugging Face

CORSI RILEVANTI

- **Security Verification and Testing:** valutazione delle vulnerabilità, penetration testing, analisi statica del codice.
- **Information Systems Security:** attacchi e analisi del rischio, PKI, IPsec, TLS, SSH, firewall e IDS, VPN.
- **Cybersecurity:** autenticazione federata (SAML, OIDC), Trusted Execution Environment, analisi forense.
- **Data Protection, Privacy and Anonymity:** gestione di identità e accessi, anonimizzazione, reidentificazione.
- **AI and Cybersecurity:** deep learning, rilevamento delle anomalie, classificazione del traffico.
- **Cryptography:** AES, RSA, SHA-3, firme digitali, ECDH, programmazione crittografica in C e Python.
- **Computer Network Technologies and Services:** progettazione di reti IPv4/IPv6, routing Internet, VPN, MPLS.

LINGUE

Uzbeko (madrelingua), russo (C1), inglese (B2), italiano (B1)