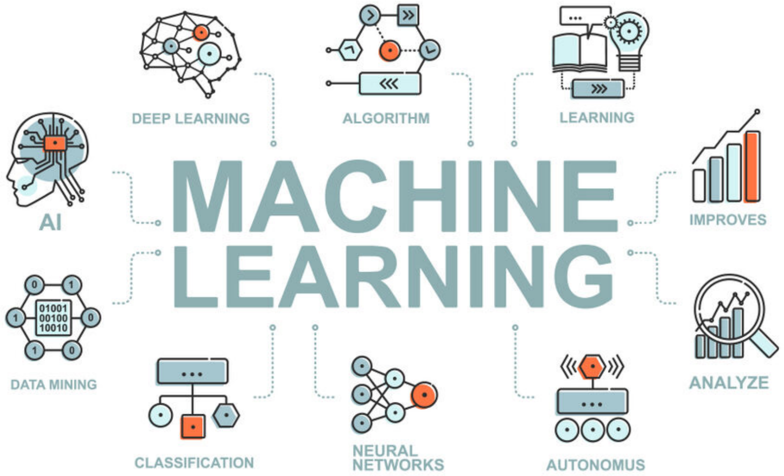
OE NIK SOC bővítésének előkészítése UBA/UEBA rendszerrel

Pardi Imre – kiberbiztonsági mérnök MSc hallgató

2023. november 5.

Mi a User and Entity Behavior Analytics (UEBA)?

- User and entity behavior analytics (UEBA), vagy user behavior analytics (UBA)
  - kiberbiztonsági megoldás
  - viselkedéselemzést, gépi tanulást használ

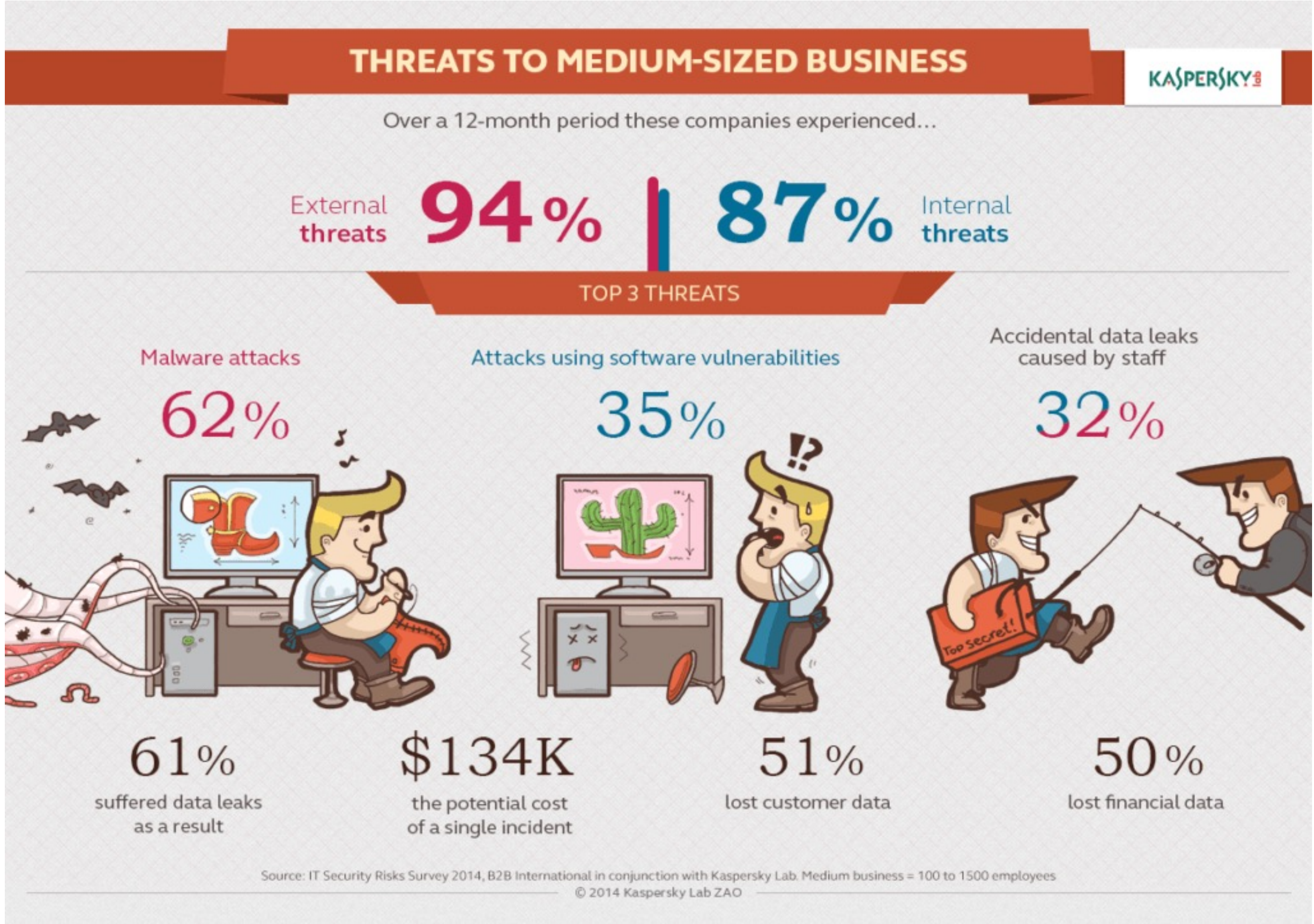


- Az UEBA – ezt a kifejezést először a Gartner 2015-ben használta – a felhasználói viselkedéselemzés (UBA) továbbfejlesztése.

Miért van szükségünk az UEBA-ra?

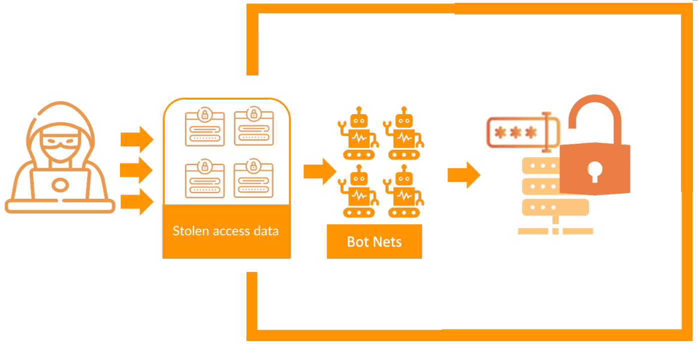
- SaaS, a felhők, hibrid rendszerek, mobilalkalmzások megjelenése

- Máshogy működik, mint a SIEM platformok
- Egyaránt foglalkozik a külső és belső fenyegetésekkel

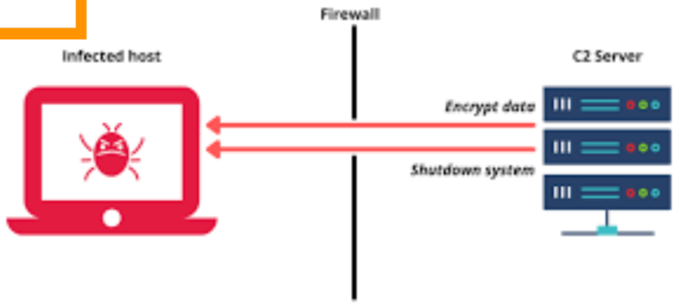


Az UEBA taktikai felhasználása

- Rosszindulatú bennfentes felhasználók



- Feltört bennfentes felhasználók



- Kompromittált entitások

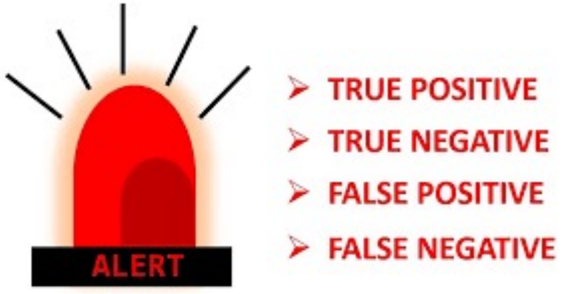
- Adatlopások kiszűrése

Az UEBA stratégiai felhasználása

- Zero Trust biztonság megvalósítása

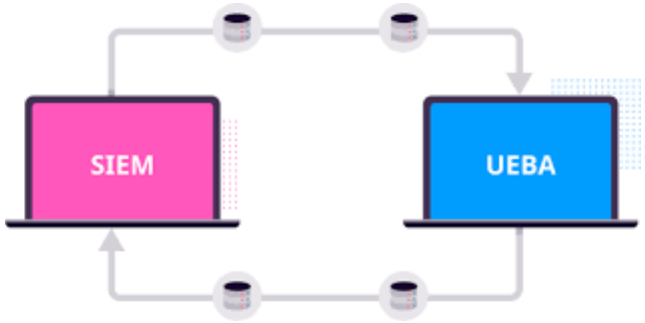
- GDPR-megfelelés

Az UEBA előnyei és hátrányai



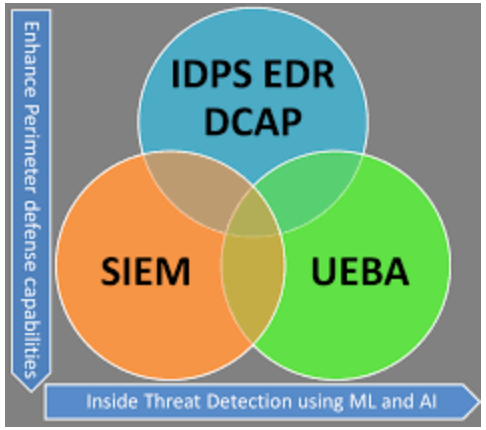
UEBA előnyök:

- Az analitikát és az adattudományt alkalmazva feltárja a biztonsági fenyegetéseket
- Az összes felhasználó és egyéb entitás nyomon követése
- Csökkenti a biztonsági eseményeket
- Kevesebb false pozitív riasztás

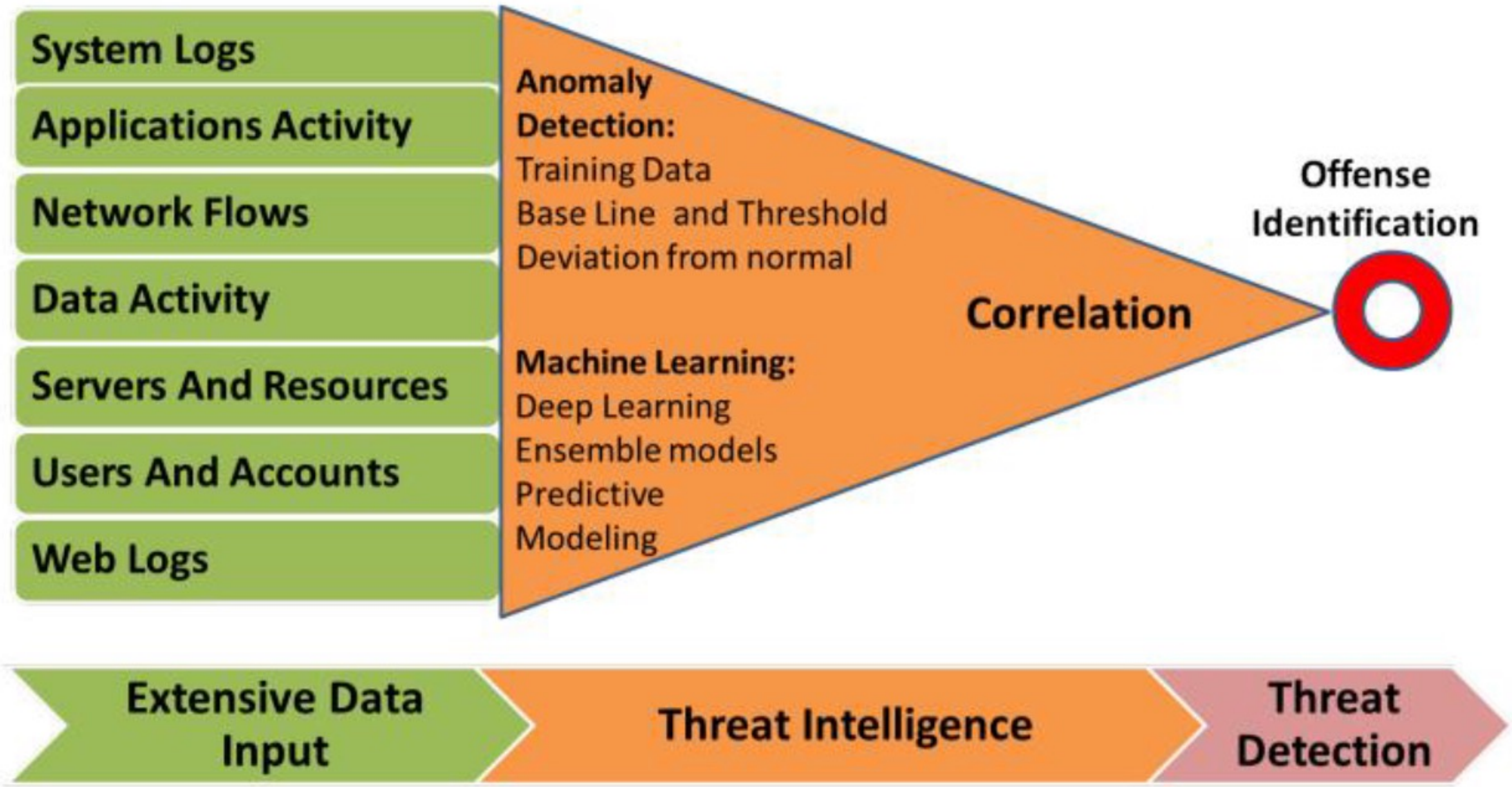


UEBA hátrányok:

- Drága a bevezetése.
- Önmagában nem elég, az SIEM, IDS/IDP, EDR/XDR eszközöket nem váltja ki.
- Harmadik féltől származó naplókat használ
- Lassan telepíthető
- Sok keresztfunkcionális jóváhagyást és rendszerkonfigurációt igényel



Az UEBA rendszer munkafolyamata



Milyen kereskedelmi vagy nyílt forráskódú UEBA eszközök érhetők el?

Önálló kereskedelmi megoldások:

- Aruba IntroSpect
- Fortinet FortiInsight
- Gurucul Risk Analytics
- Splunk-Caspida
- Securonix Bolt
- Microsoft Sentinel

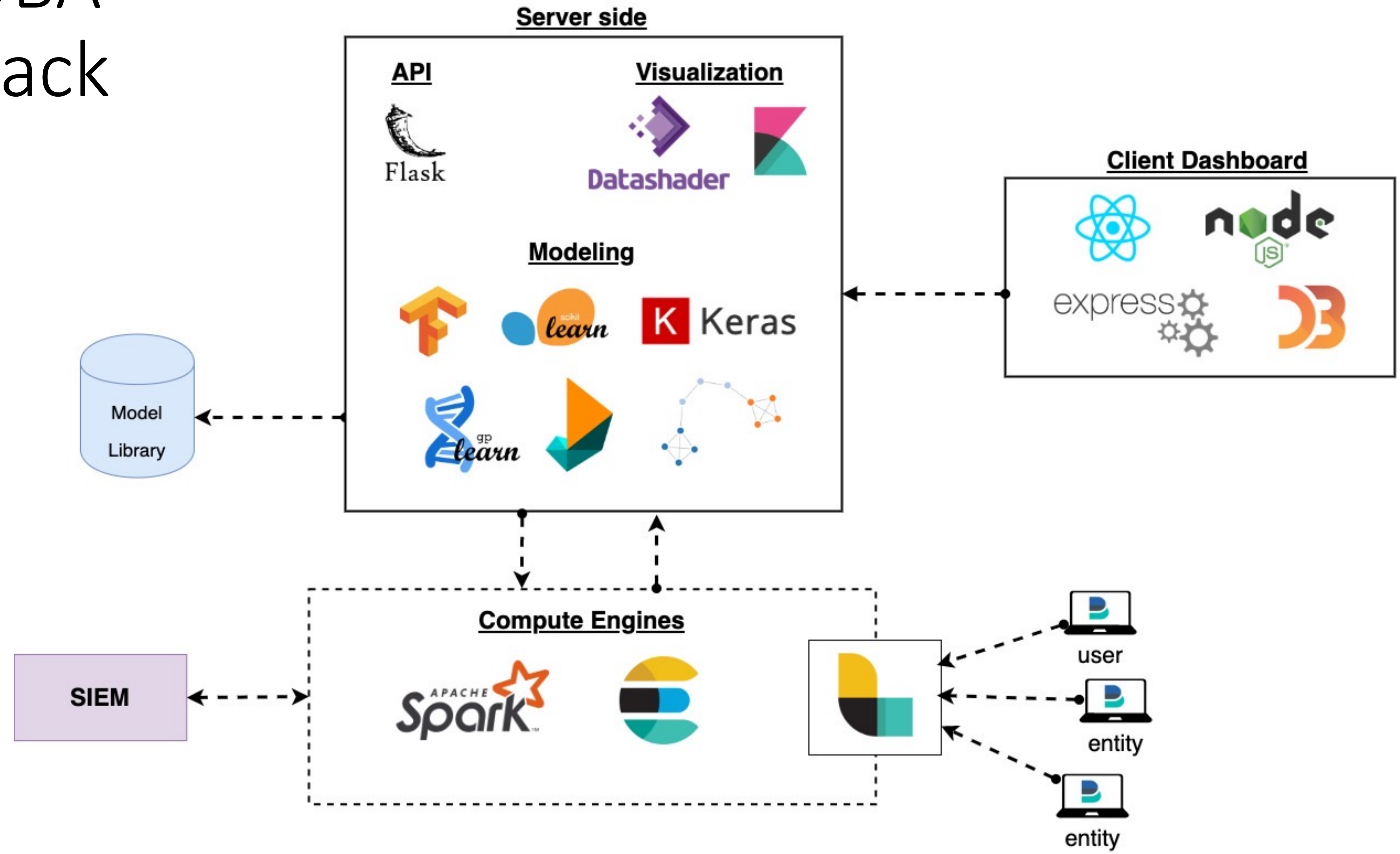
Open source megoldások:

- a piacvezető SIEM megoldások (AlienVault OSSIM, ELK Stack, SIEMMonster) még nem rendelkeznek UEBA modullal
- OpenUBA (?)

Vendor / Solution	Diverse Data Sources	Agent / Agentless	ML and AI	Risk Scoring	Key Features / Use Cases
Aruba Introspect	Yes	Agentless	100+ supervised and unsupervised ML models	Yes	Security Policy Management, Enterprise Scale SIEM Compatible, Billions of events per day
Fortinet FortiInsight	Yes	zero-config Agent	ML and AI	No	PIM, Insider Fraud, Forensic-level Reporting Regulatory Compliance Support
Gurucul Risk Analytics	Yes	Both Agent And Agentless	1000+ ML and AI Models	Yes	Self-Auditing, Account and Identity Management, signature less technology
Securonix Bolt	Yes	Agentless	Advance ML	Yes	Predictive and adaptive learning, 1000+ Threat Models, Threat Exchange library

OPEN SOURCE SIEM	KEY FEATURES	UEBA FUNCTIONALITY	LIMITATIONS
Alien Vault OSSIM	• Asset discovery • Agent and Agent less monitoring • Secure log management • Vulnerability assessment • SIEM event correlation • Host Intrusion detection system	• No UEBA functionality • No integration with other UEBA solutions	• Normalized log not available • Scalability issues • Limited log management • Can be deployed on a single server only
ELK Stack	• Utilizes three open source projects (Elasticsearch, Logstash, Kibana) • Advance log analytics • Time-series database and indexing	• No UEBA functionality • No integration with other UEBA solutions	• No threat intelligence and correlation rules • No secure log collection and management • No vulnerability scanner
SIEMonster	• ELK stack incorporated with threat intelligence and correlation rules	• UEBA functionality only available in paid version	• No machine learning and threat prevention functionality

OpenUBA tech stack



Köszönöm a figyelmet!

Források:

- https://www.ibm.com/topics/ueba (letöltve 2023. 11. 05.)
- https://www.paloaltonetworks.com/cyberpedia/what-is-ueba (letöltve 2023.11.08.)
- Tanya Akutota, Swarnava Choudhury: Big Data Security Challenges: An Overview and Application of User Behavior Analytics - International Research Journal of Engineering and Technology (IRJET)- Volume: 04 Issue: 10 | Oct -2017
- Salman Khaliq, Zain ul Abideen Tariq, Ammar Masood: Role of User and Entity Behavior Analytics in Detecting Insider Attacks – IEEE Xplore