**ZOZNAM POUŽITÝCH SKRATIEK**

|  |  |  |
| --- | --- | --- |
| **ID** | **SKRATKA** | **POPIS** |
| 1. | API | Application programming interface (rozhranie pre programovanie aplikácií) |
| 2. | Alerts | Z pohľadu IT ponímania alarm, ktorý poskytuje varovanie, výstrahu v predstihu činnosti |
| 3. | CSIRT / CSIRT.SK | Computer Security Incident Response Team Slovakia |
| 4. | CSV, STIX, MISP format | Comma-separated values; Structured Threat Information Expression (Vstupné a výstupné formáty požadované pre Open Source Platformu MISP) |
| 5. | CVEs | Common Vulnerabilities and Exposures (Referenčná metóda pre verejne známe zraniteľnosti a riziká v oblasti bezpečnosti informácií) |
| 6. | DNS | Dynamický nákupný systém |
| 7. | EU | European Union (Európska únia) |
| 8. | FortiSOAR | Holistické riešenie bezpečnostnej orchestrácie, automatizácie a odozvy (SOAR), ktoré umožňuje tímom bezpečnostných operácií urýchliť reakciu na incidenty. |
| 9. | Grace Period | Ochranná lehota - obdobie medzi koncom fakturačného cyklu a dátumom splatnosti platby. Počas tejto doby nie sú účtované úroky, pokiaľ celý zostatok je následne zaplatený do dátumu splatnosti. |
| 10. | HTTPS | Zabezpečený hypertextový prenosový protokol |
| 11. | IOC, IOCs | Indicator of compromise (Indikátori kompromisu z pohľadu počítačovej forenznej techniky) |
| 12. | ITVS | Informačná technológia verejnej správy |
| 13. | MFA | Multi Factor Authentication (Viacfaktorové overovanie) |
| 14. | MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| 15. | MISP | Malware Information Sharing Platform (Platforma na zdieľanie, zhromažďovanie, spoluprácu, ukladanie a širokú distribúciu informácií o bezpečnostných hrozbách a indikátorov kompromisu (IOC).) |
| 16. | MITRE Matrix | Predstavuje kategorizáciu a rámec na pochopenie rôznych taktík, techník a postupov (TTP), ktoré útočníci používajú počas kybernetického útoku. |
| 17. | OVM | Orgán verejnej moci |
| 18. | Qradar | IBM SIEM riešenie ktoré konsoliduje protokoly udalostí z tisícov zariadení rozmiestnených v sieti |
| 19. | RBAC | Role Based Access Control (Riadenie a mechanizmus prístupu na základe rolí a privilégií) |
| 20. | REST | Representational State Transfer (Internetový protokol, ktorý pojednáva o volaniach medzi servermi pomocou jednoduchého HTTP prenosového protokolu) |
| 21. | RFI, request RFIs | Request from information (Formát, formáty používané na zhromažďovanie informácií) |
| 22. | SaaS | Software as a service (Softvér ako služba) |
| 23. | SIEM | Security Incident and Event Managment (Systém pre management bezpečnostných informácií a udalostí, je to monitorovací a auditný nástroj) |
| 24. | SDLC | Software Development Life Cycle (Životný cyklus vývoja softvéru) |
| 25. | SOC | Security Operations Center (Bezpečnostné Dohľadové Centrum) |
| 26. | SSO | Single Sign-On (Jednotné prihlásenie) |
| 27. | SR | Slovak Republic (Slovenská republika) |
| 28. | STIX/TAXI | Structured Threat Information eXpression; Trusted Automated eXchange of Intelligence Information (Štandardy týkajúce sa nastavení ohľadom prenosu informácií o hrozbách medzi IT bezpečnostnými a spravodajskými technológiami) |
| 29. | SW | Softvér |
| 30. | TA | Trojan Agent (Vysokorizikový vírus typu trójskeho koňa používaný na šírenie škodlivého softvéru) |
| 31. | Tenable | Výrobca/Tvorca softvéru na skenovanie zraniteľnosti Nessus |
| 32. | TIP | Threat Intellingence Platform (Platforma, knižnica informácií o kybernetických hrozbách, analýze hrozieb a posudzovania hrozieb) |
| 33. | TL | Threat Library (knižnica informácií o kybernetických hrozbách) |
| 34. | TTPs | Tactics, Techniques, and Procedures (Taktika, techniky a postupy (TTP) sú kľúčovým konceptom v oblasti kybernetickej bezpečnosti a spravodajstva o hrozbách.) |
| 35. | VIP | Very important person (zameranie a funkcionalita platformy na silno exponované osoby v SVK priestore, veľmi dôležité osoby) |
| 36. | WFs, WFs on alerts | Web Files Alerts (Upozornenia na webové súbory) |