1.5. Scopul, obiectivele, principalele activităţi, rezultatele preconizate şi cerinţele specifice de realizare ale proiectului

1.5.1. Scopul şi obiectivele proiectului

(1) Scopul proiectului este consolidarea securităţii naţionale prin finanţarea de activităţi CDI ce oferă soluţii pentru necesităţi identificate la nivelul Serviciului Român de Informaţii.

(2) Obiectivul general al proiectului este:

Dezvoltarea unei aplicaţii de securitate cibernetică care utilizează algoritmi specializaţi de învăţare automată nesupravegheată şi analiză comportamentală sau mecanisme complexe de inteligenţă artificială pentru a monitoriza traficul de date din cadrul unei infrastructuri IT&C.

(3) Obiectivele specifice ale proiectului sunt:

1. Sistemul trebuie să analizeze o reţea informatică, să înveţe comportamentul reţelei şi să genereze un model de comportament pentru fiecare dispozitiv, astfel încât să poată detecta activităţile anormale (generate de aplicaţiile tip malware/trojan).
2. Sistemul monitorizează şi analizează:
   - Traficul de reţea direct către Internet (inbound/outbound);
   - Traficul de reţea către Internet (inbound/outbound) care trece prin noduri de reţea intermediare de tip servere Proxy;
   - Traficul de reţea asociat protocoalelor DNS şi DHCP;
   - Traficul de reţea din reţeaua LAN internă generat la accesarea unor aplicaţii sau servicii;
   - Traficul de reţea din reţeaua LAN internă generat în procesul de autentificare a staţiilor de lucru/serverelor la serverul de domeniu (Domain Controller);
   - Orice alt trafic de reţea generat între oricare dispozitive din reţeaua LAN internă
3. Dezvoltarea unei aplicaţii web prin care utilizatorul poate vizualiza activitatea de analiză şi monitorizare.
4. Alertele identificate sunt afişate în interfaţa grafică în funcţie de nivelul de severitate atribuit de către echipament. De asemenea se poate alege un interval de timp pentru vizualizare.
5. Pentru fiecare dispozitiv soluţia generează şi stochează informaţii despre comportamentul dispozitivului sub forma unui istoric al conexiunilor realizate. Asupra acestui istoric de conexiuni utilizatorul poate aplica opţiuni de filtrare. De asemenea utilizatorul poate descărca conexiunile sub forma unui fişier .pcap.
6. Sistemul să utilizeze algoritmi de învăţare automată nesupravegheată (unsupervised machine learning).
7. Soluţia trebuie să poată detecta următoarele tipuri de activităţi şi comportamente, prin mecanisme specifice (machine learning, analiză comportamentală):
   - Conexiuni interne şi externe
   - Transfer de date intern şi extern
   - Dispozitive conectate din reţeaua internă
   - Dispozitive conectate din exterior
   - Conexiuni active din reţeaua internă
   - Conexiuni active din exterior
   - Comportament/activitate anormală a unui dispozitiv
   - Cereri DNS reuşite/nereuşite
   - Autentificări Kerberos (reuşite/nereuşite)
   - Conexiuni suspicioase de la un dispozitiv către mai multe destinaţii
   - Conexiuni SMB nereuşite/reuşite
   - Scanarea adreselor din reţea (Address scans on the network)

- Activitate minare criptomonede
- Metode folosite de aplicaţiile malware pentru mişcarea laterală
- Sistemul de operare al dispozitivelor
- Identificare servere de tip Proxy
- Transfer de fişiere EXE
- Transfer de fişiere RAR
- Transfer de fişiere cu format necunoscut/payload
- Atacuri de tip Bruteforce
- Atacuri de tip Heartbleed
- Aplicaţii specifice atacurilor de tip Advanced Persistent Threat (APT)
- Detecţia anomaliilor în utilizarea credenţialelor
- Comunicaţii cu reţeaua TOR
- Scanare de porturi
- Conectarea pe porturi non-standard sau compromiterea unui port legitim / port hijacking
- Monitorizare trafic SMTP
- Anomalii în traficul serverelor DNS (Traffic changes to DNS servers)
- Cereri DNS de tip DynDNS (DynDNS DNS requests)
- Pierdere excesivă a conexiunilor sau a pachetelor
- Certificate SSL invalide

8. Platforma trebuie să poată fi integrată cu sisteme de tip SIEM.

1.5.2. Principalele activităţi ce urmează a fi desfăşurate în cadrul proiectului şi etapizarea acestora *(calendarul proiectului START.....STOP)*:

Nr. crt.	Activitatea / acţiunea		Perioada / Termen limită
1.	Începerea execuţiei serviciilor de conducere şi realizare a proiectului, conform prevederilor contractului de finanţare		T0
2.	Documentare şi identificare soluţii pe baza ofertelor existente pe piaţa de profil		T0 + 3 luni
3.	Definirea tehnologiilor şi metodelor utilizate, precum şi formularea cerinţelor pentru soluţiile identificare	TRL 2	T0 + 6 luni
4.	Demonstrarea şi validarea soluţiilor abordate prin experimentarea unor modele de laborator care să aplice conceptele şi tehnologiile identificate în etapele anterioare	TRL 4	T0 + 12 luni
5.	Integrarea modelelor validate într-un produs preliminar care să înglobeze soluţiile parţiale demonstrate în condiţii de laborator şi urmărirea bunei funcţionări ca sistem unitar	TRL 4	T0 + 16 luni
6.	Testarea produsului preliminar	TRL 5	T0 + 18 luni
7.	Identificarea bug-urilor şi corectarea acestora.		T0 + 19 luni
8.	Testarea finală	TRL 7	T0 + 20 luni
9.	Încheierea execuţiei complete a serviciilor prevăzute în contractul de finanţare, finalizarea realizării proiectului şi prezentarea rezultatelor cercetării		T0 + 20 luni *(20 luni de la START)*

1.5.3. Rezultatele proiectului

Rezultatele activităţilor de cercetare - dezvoltare obţinute în baza derulării contractului de finanţare pentru conducerea şi realizarea proiectului ***„Instrumente automate de detecţie a***