Objekti

Për të siguruar mbrotjen e sistemit informatik, OST sh.a. ka të implementuar një sistem për parandalim të viruseve dhe programeve të dëmshme. Ky sistem është i ndërtuar për të funksionuar në mënyrë të centralizuar në formatin *server-client* dhe i aftë për të ndërtuar politika të përgjithshme të parandalimit, monitorimit, kontrollit të viruseve si dhe të kontrollit të përdorimit te pajiseve të jashtme si USB të cilat përbëjnë një rrezik të lartë infektimi si dhe të rrjedhjes së infromacionit

Parandalimi i humbjes së të dhënave është një nga mjetet më të rendesishme te sigurisë së informacionit. OST sh.a. është një korporatë e një rëndësie të vecantë në nivel kombëtar dhe ndërkombëtar ku trajton një sasi shumë të madhe të dhënash sensitive. Të dhëna të cilat jane sensitive, individuale, kontraktore, institucionale dhe ndërkombëtare. Si të tilla këto të dhëna duhet të klasifikohen, mbrohen dhe ruhen sipas standarteve me të mira në fushën e sigurisë së informacionit. Për të mundësuar këte OST sh.a. kërkon të rinovoj liçensën së sistemit egzistues antivirus Check Point SandBlast Agent për 350 përdorues të cilët duhet të menaxhohen nga një server qëndror dhe për 50 përdorues të cilët menaxhohen nga një platformë në cloud.

Qëllimi

Rritja e shkeljeve të shkaktuara nga malware, ransomware dhe sulme të sofistikuara të inxhinierisë sociale ka bërë që perdoruesit fundore të jenë një pikë hyrëse e përhapur për kërcënimet ndaj kompanive. Këto sulme mund të jenë të fshehura në përmbajtjen e shkarkuar në internet, bashkëngjitur ne postën elektronike, pajisjet e memorjes së jashtme lëvizshme ose nga shprendarjet ne rrjet. Punonjesit pa vetedije, mund të bëhen viktima të sulmeve të tilla duke rezultuar në humbje të konsiderueshme financiare, thyerje e sigurisë së të dhënave dhe e humbjes së produktivitetit. Edhe veprimet me të thjeshta të punonjësve tuaj në ripërdorimin e kredencialeve dhe fjalekalimeve të kompanisë për veprime që nuk kanë lidhje me biznesin mund të vere komaninë përballe riskut. Më tej, me shtimin e numrit të punonjësve të cilët përdorin pajisjet e shoqërise me kontroll në distance dhe me shtimin e kontraktorëve dhe konsulentëve të cilët sjellin sistemet e tyre në shoqëri, kriminelët kibernetik i etiketojnë dobësitë në sigurinë e perdoruesit fundor për tu infiltruar dhe infektuar sistemet e këtyre punonjësve.
Për të parandaluar rritjen e rreziqeve të mundshem, duhet të realizohet rinovimi i licensës së sistemit egzistues antivirus Check Point SandBlast.

Infrastruktura aktuale

Sistemi antivirus është i instaluar në Desktop si dhe Laptop. Pajsijet të tipit laptop kanë të instaluar një sistem të qëndërzuar i cili menaxhohet në *cloud* dhe bëjnë të mundur dhe enkriptimin e plotë të diskut (*full disc encryption*).
Kontraktori duhet të realizoje rinovimin e licensës për 300 përdorues me një afat kohëzgjatje 2 vjet. Gjithashtu kontraktori duhet të realizoje njelloj rinovimin e licensës për 50 përdorues, sistem i cili aktualisht menaxhohet në cloud.

Në momentin e levrimit, licensa duhet të lëvrohet jo vetëm në hardcopy por edhe në rruge elektronike si dhe nëpërmjet portalit të prodhuesit të sistemit antivirus CheckPoint. Kontraktori duhet të bëjë një analizë/vlerësim të politikave të sistemit të antivirus të implementuara, pas këtij vleresimi, nëse është e nevojshme kontraktori duhet të propozoj/implementoj politika të tjera shtesë bazuar në praktikat më të mira të sistemeve antiviurs sipas azhornimeve më të fundit nga prodhuesi i sistemit .

Pershkrimi Teknik	
Funksionalitetet bazë të sistemit antivirus aktual	- Anti-malware - Anti-Ransomware - Anti Bot and Url Filtering
	- Threat Emulation and Anti Exploit - Media Encryption and Port Protection - Firewall and Application Controll - Zero-Phishing
	- Patch Assessment - SandBlast Agent - multiple platform support (Windows/Mac) - Host Intrusion Prevention (HIPS)

Karakteristikat e detajuara të sistemit aktual Antivirus:

Pershkrimi Teknik	
Karakteristikat e detajuara të sistemit aktual	- **Threat Emulation**: Teknologji e perparuar rezistente - **Threat Extraction**: Skanon te gjitha filet e perdoruesit ne kohe reale - **Anti-ransomware:** Parandalon dhe reagon ndaj sulmeve Ransomeware - **Zero-Phishing:** Bllokon webfaqet mashtruese dhe te njofton kur riperdoret fjalekalimi - **Anti-Bot**: Indentifikon dhe reagon ndaj host-eve te infektuara - **Anti-Exploit:** Mbron aplikacionin nga sulmet ndaj pikave te dobta te tij. - **Behavioral Guard**: Gjen dhe bllokon veprimet sulmuese ndaj perdoruesit - **Endpoint Antivirus:** Mbrotje ndaj viruseve te njohura - **Forensics:** Ruan dhe analizon cdo ngjarje per te siguruar mbrotjen maksimale ndaj sulmeve

Pershkrimi Teknik	
Analizimi i veprimeve te ndodhura	Procesi i testimit fillon automatikisht analizimin e ngjarjes sulmuese të ndodhur duke përdorur një kombinim të algoritmeve të përparuara dhe një analizë të thellë të të dhënave të papërpunuara qe jane mbledhur, ajo ndërton një përmbledhje të plotë të incidenteve. Permbledhja përbëhet nga një përshkrim i detajuar të sulmuesit, ku perfshihen: **Malicious events** – Cfarë informacionesh janë mbledhur gjatë gjithë procesit të sulmit të ndodhur **Entry point** –Si mundi virusi të hyj në rrjet. Cilat ishin elementet kryesorë që u përdorën për këtë sulm kibernetik. Si filloi sulmi. **Damage scope** –Cfarë bëri virusi që nga momenti I aktivizimit të tij? Cfare problemesh mund ti sillte koorporates. Cilat ishin të dhënat që mund të merrte. **Infected hosts** – Kush ose cfare mund të jetë infektuar tjeter. Kjo gjitheperfshirje per te gjetur ne menyre korrekte dhe te detajuar informacione mbi sulmin qe kemi marre mund te permiresohet. Administratorët e sistemit dhe ekipet e mbrojtjes ndaj sulmeve mund ti trajtojne në mënyrë efikase dhe ti zgjidhin sulmet, duke e rikthyer komanine tuaj ne gjendjen per te vazhduar punen. Me anen e SmartEvent, koorporata juaj do te jete ne gjendje ti shohe te permbledhura ne raporte te gjitha eventet e ndodhura gjate punes se kryer. Këto raporte ofrojnë analizë të sakte të incidenteve, duke përshpejtuar procesin e të kuptuarit të ciklit jetësor të plotë të sulmit dhe demtimet qe jane shkaktuar gjate tij.

Lëvrimi

NR	PËRSHKRIMI	NJËSIA	SASIA
1	Rinovim i liçensës të sistemit antivirus Check Point SandBlast Agent (350 përdorues)	Cope	1
2	Rinovim i liçensës të sistemit antivirus Check Point SandBlast Agent (50 përdorues)	Cope	1
4	Instalimi dhe konfigurimet e avancuara online dhe ne vend	Cope	1
	Vlerësim/Analize/Përmisim i politikave	Cope	1

Vendodhja:

- *Zyrat qëndore të OST sh.a. Autostrada Tirane – Durres, km 9, Kashar, Tirane, Shqiperi.*
- *Njesia Operacionale Tirane*
- *Njesia Operacionale Burrel*
- *Njesia Operacionale Shkoder*
- *Njesia Operacionale Fier*
- *Njesia Operacionale Korce*
- *Njesia Operacionale Elbasan*
- *Njesia e Mirembajtjes te Transmetimit, Tirane*