

შპს სოკარ ენერჯი ჯორჯია

მისამართი: საქართველო, თბილისი, 300 არაგველების ქ.24, 0144

სატენდერო განცხადება

1. ზოგადი ინფორმაცია

შპს სოკარ ენერჯი ჯორჯია (შემდგომში — „შემსყიდველი“) აცხადებს ტენდერს საფრთხეების ანალიზის პატფორმა - SOCRadar-ის შესყიდვაზე და იწვევს დაინტერესებულ პირებს (შემდგომში — „პრეტენდენტები“) წარმოადგინონ სატენდერო წინადადება წინამდებარე დოკუმენტში მითითებული პირობებისა და მოთხოვნების შესაბამისად.

შესყიდვის საგანია: საფრთხეების ანალიზის პატფორმა - SOCRadar შეძენა, მე-3 პუნქტში განსაზღვრული რაოდენობითა და ტექნიკური მახასიათებლებით.

2. შემსყიდველის რეკვიზიტები

- დასახელება: შპს სოკარ ენერჯი ჯორჯია
- საიდენტიფიკაციო კოდი: 202349440
- იურიდიული/ფაქტობრივი მისამართი: საქართველო, თბილისი, 300 არაგველების ქ.24, 0144
- საკონტაქტო პირი: ლაშა-გიორგი ჭელიძე
- ტელეფონი: +995 591517302
- ელ. ფოსტა: l.chelidze@socar.ge

3. შესყიდვის საგანი და ტექნიკური მოთხოვნები

ქვემოთ მოცემულია შესასყიდი საქონლის ჩამონათვალი მინიმალური ტექნიკური მახასიათებლებით.

საფრთხეების ანალიზის პატფორმას უნდა გააჩნდეს შემდეგი მოდულები (ასევე აკმაყოფილებდეს შემდეგ მოთხოვნებს):

1. CTI & Supply Chain Intelligence

- პლატფორმას უნდა გააჩნდეს საძიებო ინსტრუმენტი IP-მისამართის, დომენის, ჰეშის, ელფოსტის, URL-ისა და საკვანძო სიტყვების მიხედვით ძიებისთვის, შიდა სისტემებთან ინტეგრაციისა და შესაბამისი რისკის საკითხების დაყენების შესაძლებლობით.
- პლატფორმამ უნდა უზრუნველყოს დამატებითი მონაცემები, როგორიცაა Jarm Hash, Header Hash, WHOIS მონაცემები, DNS ჩანაწერები და SSL სერტიფიკატების ინფორმაცია დომენზე დაფუძნებული საფრთხის მოძიებისთვის.
- პლატფორმამ უნდა შესაძლებელი გახადოს ძიება 50-ზე მეტ წყაროზე — მათ შორის მესენჯერებზე, სოციალურ ქსელებზე, ბნელი ქსელის ბაზრებზე, საფრთხის ფიდებზე, API-კოლექციის პლატფორმებსა და კოდის რეპოზიტორიებზე — ენობრივი შეზღუდვების გარეშე, მათ შორის Discord, BlueSky, GitHub Gist, Repo Activity და Hugging Face.
- პლატფორმას უნდა შეეძლოს სპეციალიზებული და პერსონალიზებული ძიებების შენახვა კონკრეტული პარამეტრებით, რომელთა შესრულებაც შესაძლებელი იქნება რეგულარულ ინტერვალებში, ასევე ლოგიკური ოპერატორების (AND, OR, NOT) გამოყენებით რთული მოთხოვნების ფორმირება.
- პლატფორმას უნდა შეეძლოს ინტელექტუალური ძიების ჩატარება InfoStealer-ისა და მონაცემთა გაჟონვის ბაზებში დომენის, Stealer ID-ის, URL-ისა და მომხმარებლის სახელის მიხედვით, ასევე ორგანიზაციის მომხმარებლების/თანამშრომლების მიხედვით ფილტრაციის შესაძლებლობით.
- Stealer ლოგებში წარმოდგენილი უნდა იყოს დეტალური ინფორმაცია, მათ შორის შესაძლო მომხმარებლები/თანამშრომლები, IP მისამართები, HWID, GUID, მომხმარებლის სახელი, პაროლები, პაროლის ჰეშები, NTLM ჰეშები, ფაილების სტრუქტურა, Stealer-ის ოჯახი, მოწყობილობის ინფორმაცია, ოპერაციული სისტემა, ქვეყანა, მავნე ფაილის მდებარეობა, დროის სარტყელი, UAC ტიპი და ანტივირუსის ინფორმაცია.
- პლატფორმამ AI-ზე დაფუძნებული ანალიზით უნდა გამოკვეთოს იდენტობის რისკის სრული პროფილი, მათ შორის მესამე მხარის სერვისებში ავტორიზაციის მონაცემების გამჟღავნება.
- პლატფორმას უნდა გააჩნდეს 130-ზე მეტი საფრთხის ფიდი OSINT, საკუთარი და კომერციული წყაროებიდან, ექსპორტის შესაძლებლობით JSON, CSV, RAW და TEXT ფორმატებში, ასევე წვდომით Endpoint API, MISP და TAXII სერვერების მეშვეობით.

- საფრთხის ფიდის მონაცემები დღეში უნდა შეიცავდეს 75 000-ზე მეტ ახალ IOC-ს, მათ შორის ბოტნეტების IP მისამართებს, კიბერ საკომანდო-საკონტროლო სერვერების IP-ებს, ყალბ დომენებს, APT ჯგუფებთან დაკავშირებულ IP-მისამართებსა და ცნობილი მავნე პროგრამების ჰეშებს.
- პლატფორმას უნდა შეეძლოს პერსონალიზებული კოლექციების შექმნა დახვეწილი ფილტრებით, ცრუ დადებითი შედეგების შესამცირებლად, ისეთი პარამეტრებით როგორიცაა ქვეყანა, IOC-ის ტიპი, IOC ქულის მინიმალური/მაქსიმალური ზღვარი და სხვ.
- პლატფორმას უნდა შეეძლოს გაფილტრული IOC-ების ექსპორტი ზემოაღნიშნულ ფორმატებში SIEM/SOAR/Firewall სისტემებში, DDoS, DNS გაძლიერების და ფიშინგის შეტევებისგან ავტომატური დაცვისთვის.
- პლატფორმას უნდა შეეძლოს მაღალი ხარისხის ფიდების მიწოდება კონკრეტული სექტორების, რეგიონებისა და მიმდინარე გლობალური თავდასხმის კამპანიების მიხედვით.
- პლატფორმას უნდა შეეძლოს IOC-ზე დაფუძნებული სიღრმისეული გამოძიების ჩატარება — საფრთხის აქტორის წარმომავლობის, სამიზნეების, IOC-ურთიერთკავშირების ვიზუალიზაციისა და ისტორიული ანალიზის მიმართულებით, IOC-ების მასობრივი ატვირთვის შესაძლებლობით.
- პლატფორმას უნდა შეეძლოს დამნაშავეთა ფორუმებსა და საიტებზე მონაცემთა გაჟონვასთან დაკავშირებული პოსტების თვალის დევნება და ფილტრაცია ქვეყნის, ინდუსტრიის, საფრთხის აქტორისა და კატეგორიის მიხედვით.
- პლატფორმამ უნდა უზრუნველყოს 100-ზე მეტი ფაილის ფორმატის სტატიკური და დინამიკური მავნე პროგრამების ანალიზი, დეტალური ანგარიშით, რომელიც მოიცავს ქცევის ანალიზს, MITRE ATT&CK რუკირებას, პროცესების ხეს, შესრულებულ ბრძანებებს, მავნე პროგრამის ოჯახს, საფრთხის აქტორის კონტექსტს და აღმოჩენილ საეჭვო კოდებს.
- მავნე პროგრამების ანალიზის ფუნქციონალი უნდა მოიცავდეს URL-ის ანალიზს, ჰეშზე დაფუძნებული ანგარიშების მოძიებას, ასევე EML და MSG ფაილების ანალიზს ელფოსტაზე დაფუძნებული საფრთხეებისა და დანართებისთვის.
- პლატფორმას უნდა გააჩნდეს საფრთხის მოძიების წესების (Threat Hunting Rules) ცალკე დაფა დეტალური MITRE ATT&CK ნავიგატორით, 35 000-ზე მეტი YARA, Sigma, Snort და Suricata წესის მხარდაჭერით.
- პლატფორმას უნდა გააჩნდეს საფრთხის ინტელექტის სპეციალური დაფა, გლობალურ კვლევებზე დაფუძნებული, ორგანიზაციისთვის აქტუალური საფრთხეების შესახებ, საფრთხის აქტორთა/გამომძალველი ჯგუფების ინფორმაციისა და მათ მიერ აქტიურად გამოყენებული დაუცველობების შესახებ შეტყობინებით.
- პლატფორმას უნდა შეეძლოს საფრთხის აქტორების, გამომძალველი ჯგუფებისა და მავნე პროგრამების აქტიური მონიტორინგი ერთიანი ხედით, თითოეულისთვის გავლენის ქულით, საფრთხის მეტრით და დახვეწილობის დონით, 10-ზე მეტი პარამეტრით ფილტრაციის შესაძლებლობით.

- პლატფორმას უნდა შეეძლოს არჩეული საფრთხის აქტორებისა და გამომძალველი ჯგუფებისთვის მიმდინარე IOC-ების, MITRE ATT&CK-ზე დაფუძნებული TTP-ების და YARA/Sigma წესების ინფორმაციის მიწოდება პლატფორმისა და API-ის მეშვეობით.
- პლატფორმას უნდა შეეძლოს თითოეული ჯგუფისთვის შერბილებისა და მოგვარების სტრატეგიების მიწოდება, ორგანიზაციის თავდაცვის სტრატეგიის გასაუმჯობესებლად.
- პლატფორმას უნდა შეეძლოს ბნელი ქსელიდან შეგროვებული ინფორმაციისთვის (დაუცველობები, საფრთხის აქტორის ინტელექტი, გამომძალველთა ინტელექტი) AI-ზე დაფუძნებული რეზიუმეების გენერაცია.
- პლატფორმას უნდა შეეძლოს IOC-ების დაკავშირება დაფიქსირებულ თავდასხმის კამპანიებთან, მავნე ინფრასტრუქტურის რეალურ გამოყენებაზე მოცემული ხედვის მისაწოდებლად.
- პლატფორმას უნდა გააჩნდეს საფრთხის აქტორის მონაცემების კონტექსტური გამდიდრების ფუნქცია (მაგ.: ფსევდონიმები, გეოლოკაცია, სამიზნეობის ქცევა, ისტორიული თავდასხმები, დაკავშირებული მავნე პროგრამები).
- პლატფორმას უნდა გააჩნდეს დარგობრივი (მაგ.: ფინანსური, ჯანდაცვის, სახელმწიფო) დაფები სექტორული საფრთხის მონიტორინგის გასამარტივებლად.
- პლატფორმას უნდა შეეძლოს კონკრეტული თავდასხმის კამპანიებისთვის კვლევის დონის მონაცემების მიწოდება — სიღრმისეული ტექნიკური და უსაფრთხოების ანალიზი, ისტორიული ვადები და სრული დეტალები თავდასხმის პირველი გამოვლენიდან, პლატფორმის ცალკე მონაკვეთში.
- პლატფორმას უნდა შეეძლოს, შესაძლებლობის ფარგლებში, მილიონობით მესამე და მეოთხე მხარის კომპანიის მონიტორინგი და გლობალურ ტენდენციებზე სიღრმისეული ანალიზის ჩატარება, რათა გენერირდეს ადრეული გაფრთხილება, როდესაც მესამე მხარის მომწოდებელი განიცდის უსაფრთხოების ინციდენტს ბნელი ქსელის ან ღია წყაროს მონაცემებზე დაყრდნობით.
- პლატფორმას უნდა გააჩნდეს მაღალი დონის დაფა, რომელიც ეხმარება მიმწოდებელთა თვალის დევნებას წარმოქმნილი საფრთხეების მიხედვით, პოზიციის ცვლილებების მონიტორინგს რეალურ აქტივობაზე დაყრდნობით და გეოგრაფიულ/ინდუსტრიულ საერთო რისკების იდენტიფიცირებას.
- მაღალი დონის დაფა უნდა მოიცავდეს: თავდასხმის ვადებს, რისკის ქულის განაწილებას, ძირითად ინდიკატორებს გამოძიების საწყისი წერტილებისთვის, ყველაზე მაღალი რისკის მქონე კომპანიების სიას, უახლეს ამბებსა და აქტივობებს, ასევე მესამე მხარის გლობალური მომწოდებლების გეო-რუკირებას.
- პლატფორმას უნდა გააჩნდეს მომწოდებელთა პროფილების მიმოხილვისთვის ცალკე მონაკვეთი, რომელიც წარმოაჩენს ორგანიზაციის მომწოდებლებთან უშუალოდ დაკავშირებულ რისკებსა და გამჟღავნებებს, პრიორიტეტების დადგენით გამოყენების, პოპულარობისა და შესაბამისობის მიხედვით — მინიმუმ შემდეგი პარამეტრებით: აპლიკაციის უსაფრთხოება, ღრუბლოვანი უსაფრთხოება, კონფიდენციალური

ინფორმაციის გამჟღავნება, კიბერდანაშაულის ეკოსისტემა, DNS-ის მდგომარეობა, ელფოსტის უსაფრთხოება, IP/დომენის რეპუტაცია, ქსელის უსაფრთხოება, თავდასხმის ქვეშ მყოფი ორგანიზაცია, კოდის რეპოზიტორია, SSL/TLS უსაფრთხოება და დაუცველობების მონიტორინგი.

- პლატფორმას უნდა გააჩნდეს რისკის განსაზღვრის დახვეწილი მეთოდი თითოეული მომწოდებლისთვის, 100-ზე მეტი შემოწმებით გარე რისკების, მონაცემთა გაჟონვისა და საფრთხის ინტელექტის შესახებ, მონაცემებზე დაფუძნებული მომწოდებლის ქულის მისაცემად.
- პლატფორმას უნდა გააჩნდეს გლობალური ტენდენციების მონიტორინგის დაფა, რომელიც აერთიანებს საფრთხის ანგარიშებს, გაჟონვების განახლებებსა და დაუცველობების გამოვლენას, ქვეყნისა და ინდუსტრიის ტენდენციებით, თავდასხმის ტენდენციებით, კომპანიის მიმოხილვითა და რისკის სურათით, AI ანალიტიკითა და სიახლეების ანალიზით.
- პლატფორმას უნდა შეეძლოს მოთხოვნით შეფასებების გენერირება, კონკრეტული მომწოდებლების სწრაფად ხელახლა შესაფასებლად ან ბოლოდროინდელი ცვლილებების დასადასტურებლად.

2. Digital Risk & Dark Web Monitoring

- პლატფორმას უნდა გააჩნდეს კონფიგურაციული მოქნილობა — საკვანძო სიტყვების დამატება/წაშლა და კონკრეტული წყაროების არჩევა ღრმა და ბნელი ქსელის სკანირებისთვის.
- პლატფორმას უნდა შეეძლოს სხვადასხვა საკვანძო სიტყვის, IP-მისამართის, დომენის, DLP იდენტიფიკატორის, VIP ანგარიშისა და BIN ნომრების შეყვანა სხვადასხვა მონაცემთა წყაროზე ძიებისთვის.
- პლატფორმას უნდა შეეძლოს მგრძნობიარე მონაცემების იდენტიფიცირება DLP იდენტიფიკატორების გამოყენებით (IBAN, პირადი ნომერი, საიდენტიფიკაციო ან ზოგადი კოდები), მონაცემთა გაჟონვის ან არასანქცირებული გაზიარების შემთხვევაში მყისიერი განგაშის გენერირებით.
- ბოტნეტის მონაცემები, პერსონალური მონაცემები (PII), საეჭვო კონტენტი, შავი ბაზრისა და მყისიერი შეტყობინებების ინფორმაცია მარტივად ხილვადი უნდა იყოს პლატფორმაზე.
- პლატფორმას უნდა გააჩნდეს ბნელი ქსელის ისტორიული ხსენებების არქივი ანალიტიკოსებისთვის, დაჯგუფებული აქტორის, ფორუმისა და სიმძიმის მიხედვით გამოძიების მიზნებისთვის.
- პლატფორმას უნდა შეეძლოს ბნელი ქსელიდან მოძიებული მონაცემების ელფოსტით მარტივად გადმოწერა.

- პლატფორმას უნდა შეეძლოს ბნელი ქსელის მონიტორინგის მეშვეობით ორგანიზაციის თანამშრომლებსა და მომხმარებლებზე ორიენტირებული მავნე პროგრამების (მაგ.: infostealer) აღმოჩენა.
- პლატფორმას უნდა გააჩნდეს აქტივების შესაბამისი კონტროლი შავ ბაზრებზე არასასურველი ობიექტების გასაფილტრად და ცრუ დადებითი შედეგების შესამცირებლად.
- პლატფორმას უნდა შეეძლოს ინტერფეისის საშუალებით შავ ბაზარზე გასაყიდად გამოტანილი მონაცემების მარტივი შესყიდვის ხელშეწყობა, დაზარალებული მოწყობილობისა და მისი კონფიგურაციის შესახებ ინფორმაციის ჩათვლით.
- პლატფორმას უნდა შეეძლოს შავ ბაზარზე გამოტანილი, გასაყიდი გაჟონილი მონაცემების წინასწარი მიმოხილვის ეკრანის ჩვენება შესყიდვამდე.
- პლატფორმას უნდა შეეძლოს პირადი და კორპორატიული ავტორიზაციის მონაცემების გამოყენების გარჩევა (დომენის დამთხვევის ან ტეგიერების საშუალებით), ასევე გაჟონილ მონაცემებში უნიკალური FQDN-ების, პაროლებისა და მომხმარებლის სახელების გამოკვეთა.
- პლატფორმას უნდა შეეძლოს ორგანიზაციის თანამშრომელთან ან მომხმარებელთან დაკავშირებული Stealer log მონაცემების აღმოჩენა, ხელმისაწვდომობის შემთხვევაში პაროლის სირთულისა და მოწყობილობის ინფორმაციის გამოკვეთით.
- პლატფორმას უნდა შეეძლოს გასაყიდი VPN და თანამშრომელთა ანგარიშების შემოწმება.
- პლატფორმას უნდა შეეძლოს Telegram არხებში, ჰაკერულ ფორუმებზე და მესამე მხარის გაჟონებებში აღმოჩენილი თანამშრომელთა ავტორიზაციის მონაცემების აღმოჩენა და განგაშის გენერირება, თითოეული აღმოჩენისთვის წყაროს ინფორმაციის მითითებით.
- პაროლების გაგზავნის კონფიგურაცია მარტივად სამართავი უნდა იყოს პლატფორმის მეშვეობით, დაფარული და ღია ფორმატის შესაძლებლობით მოთხოვნის შემთხვევაში.
- პლატფორმას უნდა შეეძლოს ორგანიზაციის სამიზნედ ქცეული კომუნიკაციის აღმოჩენა და ანგარიშგება Telegram-ის, Discord სერვერების, IRC და ICQ არხების მეშვეობით.
- პლატფორმას უნდა შეეძლოს ორგანიზაციასთან დაკავშირებული საექვო კონტენტის შემოწმება ჰაკერულ ფორუმებზე, XSS ფორუმებზე, Exploit.in ფორუმებზე, Pastebin.pl-ზე და სხვა Paste საიტებზე, შესაბამისი განგაშის გენერირებით.
- პლატფორმას უნდა შეეძლოს ბნელი ქსელის პოსტებიდან ნიმუშური მონაცემების მოძიების ხელშეწყობა, თუ მონაცემები უფასო და გადმოსაწერია.
- პლატფორმას უნდა შეეძლოს განგაშის გენერირება VIP ანგარიშის ელფოსტის გაჟონვისას, გაჟონვის წყაროს მითითებით.
- პლატფორმას უნდა შეეძლოს VIP პირის როგორც სამსახურებრივი, ისე პირადი ელფოსტის მისამართის მონიტორინგისთვის დამატება.
- პლატფორმას უნდა შეეძლოს BIN ნომრებისა და SWIFT კოდების ძიება ბნელ ქსელში, Telegram-სა და მყისიერი შეტყობინებების პლატფორმებზე.

- პლატფორმას უნდა შეეძლოს კონფიგურირებული BIN ნომრებისთვის საკრედიტო და სადებეტო ბარათების გაჟონვის აღმოჩენა.

3. Reporting

- პლატფორმას უნდა გააჩნდეს AI-ზე დაფუძნებული ანგარიშების მართვის მოდული 15-ზე მეტი მზა შაბლონითა და მორგებული ანგარიშების ფუნქციით, რაც საშუალებას იძლევა რამდენიმე წუთში მომზადდეს ხელმძღვანელობის დონის ანგარიშები.
- პლატფორმას უნდა გააჩნდეს სისტემურად განსაზღვრული შაბლონები, რომლებიც უზრუნველყოფენ ანგარიშების სტანდარტიზებულ საწყისებს — შაბლონის სტრუქტურასა და კონფიგურაციის მოდელს, შესრულების თვალთვალთან და მასალის მთლიანობას, კონტროლირებად მონაცემთა მოდელსა და მოთხოვნების მართვას, დამტკიცებულ ფარგლებში AI-ის დახმარებით შაბლონის შექმნას და მორგებული ანგარიშების, როგორც ანგარიშების ძირითადი შრის, როლს.
- პლატფორმას უნდა გააჩნდეს მორგებული ანგარიშის სამუშაო პროცესის მმართველი, რომელიც მომხმარებელს დაეხმარება საკუთარი ანგარიშის შექმნაში სხვადასხვა თემის, გრაფიკის, მოდულური მოთხოვნისა და დიაგრამის ტიპის გამოყენებით.
- ანგარიშები ავტომატურად უნდა იგზავნებოდეს განსაზღვრულ ინტერვალებში (ერთჯერადად, ყოველკვირეულად, ყოველთვიურად ან კვირის კონკრეტულ დღეებში) მითითებულ ელფოსტის მისამართებზე პლატფორმიდან; თუ ელფოსტით მიმდგომი შეუძლებელია, უნდა გაიგზავნოს შეტყობინება ანგარიშის მომზადების შესახებ.
- პლატფორმას უნდა გააჩნდეს სპეციალიზებული Copilot აგენტი, რომელიც ეხმარება ანგარიშების ლოგიკის შექმნაში მარტივი გამოყენებისთვის.

4. Platform Management

- ინტერფეისზე წვდომა უზრუნველყოფილი უნდა იყოს დაცული არხით (HTTPS), ხოლო ვებ-ინტერფეისს უნდა გააჩნდეს ორფაქტორიანი ავთენტიფიკაცია (2FA) SMS-ის, ავთენტიფიკატორისა და ელფოსტის მეშვეობით.
- ვებ-ინტერფეისზე წვდომა შესაძლებელი უნდა იყოს მხოლოდ ორგანიზაციის მიერ განსაზღვრული IP-მისამართებიდან (whitelist მხარდაჭერით), ხოლო სხვა IP-მისამართებისთვის უნდა იყოს დაბლოკილი (IP შეზღუდვა პორტალზე წვდომისთვის).
- პლატფორმას უნდა გააჩნდეს მორგებადი დაფები სხვადასხვა მოდულის ვიჯეტებით და ხშირად გამოყენებული გვერდების ჩამაგრების საშუალება.
- პლატფორმას უნდა გააჩნდეს ჩაშენებული AI ჩატბოტი, რომელიც ეხმარება ანალიტიკოსს ყოველდღიურ ოპერაციებში რეალურ დროში დახმარებისა და მომხმარებელთა შეკითხვებზე პასუხის გაცემით.
- პლატფორმას უნდა შეეძლოს ბნელი ქსელიდან, დაუცველობებისა და განგაშებისგან შეგროვებული ინფორმაციისთვის AI-ზე დაფუძნებული რეზიუმეების გენერირება.

- პლატფორმას უნდა შეეძლოს დუბლირებული/ცრუ დადებითი მონაცემების (მაგ.: გაჟონილი ავტორიზაციის მონაცემები) მოცილება მომხმარებელი-პაროლი-FQDN პრინციპზე დაფუძნებული შემოწმებით თითოეული აღმოჩენისთვის.
- პლატფორმას უნდა გააჩნდეს განგაშების მართვის მონაკვეთი, რომელიც ინციდენტების მართვის დაფის ფუნქციასაც შეასრულებს — სიმძიმის ცვლილება, ტეგირება და გუნდის წევრზე მინიჭება ზუსტი თვალთვალთ.
- პლატფორმას უნდა შეეძლოს განგაშების მასობრივი გააქტიურება/გამორთვა, ელფოსტითა და API ინტეგრაციით შეტყობინების მიღების ვარიანტებით.
- პლატფორმას უნდა შეეძლოს მორგებული წესების კონფიგურირება ცრუ დადებითი შედეგების აღმოსაფხვრელად — მაგ.: პაროლის პოლიტიკაზე, ცარიელ მნიშვნელობებზე ან ბნელი ქსელის განგაშებზე დაფუძნებული წესები, სიმძიმისა და ანალიტიკოსზე მინიჭების მორგებული პირობებით.
- პლატფორმას უნდა გააჩნდეს AI აგენტი, რომელიც ავტომატურად სთავაზობს პირობებს ცრუ დადებითი შედეგების შესამცირებლად.
- დაგენერირებული განგაში, ინციდენტის მიხედვით, უნდა შეიცავდეს გაჟონვის წყაროს, პაროლის დეტალებს, პაროლის ტიპსა და ბმულს ნედლ მონაცემებზე წვდომისთვის, ასევე AI-ზე დაფუძნებულ რჩევებს რეაგირებისა და შერბილებისთვის.
- პლატფორმას უნდა გააჩნდეს გაფართოებული ვარიანტები ორგანიზაციის პაროლის პოლიტიკის დასამატებლად, სხვადასხვა ავტორიზაციის მონაცემთა გაჟონვის განგაშებში ცრუ დადებითი შედეგების ავტომატური მოცილებისთვის.
- პლატფორმას უნდა გააჩნდეს საჭირო ჩამრთველები მგრძნობიარე მონაცემების, ღია ტექსტის პაროლებისა და Stealer log-ის შემცველობის ანალიტიკოსებისგან დამალვისთვის, ასევე სხვადასხვა სკანირების ჩართვა/გამორთვის საშუალება.
- პლატფორმას უნდა შეეძლოს სხვადასხვა სახის ინტელექტის შეტყობინებებზე გამოწერა — ყოველდღიური მიმოხილვები, საფრთხის ანგარიშები, HUMINT ინტელექტი და სხვ.
- პლატფორმას უნდა გააჩნდეს ყველა მომხმარებლის აუდიტის ჟურნალი, რომელიც თვალყურს ადევნებს შესვლის მცდელობებსა და სხვადასხვა მოდულში/სექციაში განხორციელებულ ცვლილებებს, მინიმუმ 6 თვის განმავლობაში შენახვით.
- პლატფორმას უნდა შეეძლოს მომხმარებელთა და აუდიტის ჟურნალების ექსპორტი სტანდარტულ ფორმატებში (Excel) SIEM სისტემებთან ინტეგრაციისთვის.
- პლატფორმას უნდა გააჩნდეს მარტივად გამოსაყენებელი რესურსების მონაკვეთი, სადაც ხელმისაწვდომია პროდუქტის უახლესი განახლებების ინფორმაცია, დახმარების ცენტრი და ხშირად დასმული კითხვები.
- პლატფორმის რესურსების ცენტრს უნდა შეეძლოს პროდუქტისა და საკონსულტაციო გუნდისთვის საკითხების დაყენების საშუალების მიცემა.
- რესურსების ცენტრი ასევე უნდა მოიცავდეს ბლოგებზე, ვებინარებსა და სასწავლო პლატფორმაზე წვდომას.

5. API & Integrations

- პლატფორმას უნდა გააჩნდეს ცალკე ინტეგრაციის გვერდი წამყვან უსაფრთხოების ტექნოლოგიებთან (SIEM, SOAR, EDR, Firewall და სხვ.) მზა ინტეგრაციის შესაძლებლობით.
- პლატფორმას უნდა გააჩნდეს სხვადასხვა API ოფცია გამოყენებული მოდულების მიხედვით მონაცემების მისაღებად — ბნელი ქსელის მონაცემები (ავტორიზაციის მონაცემების გაჟონვა, შავი ბაზრის მონაცემები, საჯარო მონაცემების გამჟღავნება), დაუცველობის მონაცემები, იდენტიფიკაციისა და წვდომის ინტელექტის მონაცემები, ფიშინგის მონაცემები, კომპანიის აუდიტის ჟურნალის მონაცემები, ანგარიშები და აუდიტის ჟურნალები.
- პლატფორმას უნდა შეეძლოს Webhook-ების მხარდაჭერა თანამშრომლობის პლატფორმებთან (Slack, MS Teams) რეალურ დროში ინტეგრაციისთვის, მორგებული განგაშის მიწოდების ავტომატიზაციით.
- პლატფორმას უნდა შეეძლოს ფილტრების/წესების დაყენება, რომელი განგაშები ან მონაცემები გადაიცემა ინტეგრაციის მეშვეობით (მაგ.: მხოლოდ კრიტიკული განგაშები ან კონკრეტული მოდულები).
- პლატფორმას უნდა გააჩნდეს დეტალური API დოკუმენტაცია და სატესტო გარემო (PoC) მომხმარებლისთვის ინტეგრაციის მარტივად განსახორციელებლად.
- პლატფორმას უნდა შეეძლოს API-ის მეშვეობით საფრთხის ფიდის მონაცემების ექსპორტი უსაფრთხოების ხელსაწყოებზე ფართო ფორმატებში — Raw Text, Text, Excel, Comma Separated, JSON, TAXII და სხვ.
- პლატფორმას უნდა გააჩნდეს TAXII 2.1 სტანდარტთან თავსებადი სერვისი, სტანდარტიზებული მონაცემების (STIX) გაცვლისთვის უსაფრთხოების ხელსაწყოებს შორის.

6. Attack Surface Management

- პლატფორმას უნდა შეეძლოს ავტომატურად გამოავლინოს და ურთიერთდაუკავშიროს ორგანიზაციასთან დაკავშირებული ყველა დომენი, ქვედომენი, IP-მისამართი, მესამე მხარის დომენები, SSL სერტიფიკატები, ღია პორტები, ვებგვერდები, მობილური აპლიკაციები, API-ბოლოწერტილები და გამომჟღავნებული ღრუბლოვანი საცავები, მომხმარებლისგან დამატებითი ინფორმაციის გარეშე.
- პლატფორმას რეგულარულად უნდა შეეძლოს პასიური და აქტიური სკანირების ჩატარება ორგანიზაციის ინტერნეტში გამოვლენილი აქტივებისთვის, თავდასხმის ზედაპირის იდენტიფიცირებისა და პლატფორმაზე მათი წარმოჩენისთვის.
- პლატფორმას უნდა შეეძლოს აქტიური სკანირების კონტროლი — კონკრეტული აქტივებისთვის საჭიროებისამებრ ჩართვის ან გამორთვის მოქნილობით.
- აქტივების კლასიფიკაცია მყისიერი და ავტომატური უნდა იყოს. აქტივები მარტივად საძიებელი და კატეგორიზებული უნდა იყოს პლატფორმაზე.

- დამატებითი აქტივების ხელით დამატება ან წაშლა შესაძლებელი უნდა იყოს მარტივი ინტერფეისის მეშვეობით.
- პლატფორმას უნდა შეეძლოს აქტივების ექსპორტი ანგარიშგების მიზნებისთვის მომხმარებლის სხვა სისტემებში.
- პლატფორმას უნდა გააჩნდეს ინტერაქტიული ვიზუალური ციფრული ანაბეჭდის რუკა, რომელიც დინამიურად აჩვენებს კავშირებს აღმოჩენილ დომენებს, IP-მისამართებს, პორტებსა და სერვისებს შორის.
- პლატფორმას უნდა შეეძლოს იმ დომენების აღმოჩენა, რომლებსაც ორგანიზაცია ამჟამად აქტიურად არ იყენებს.
- პლატფორმას ავტომატურად უნდა შეეძლოს 1200-ზე მეტი ტექნოლოგიის ამოცნობა და გამოვლენა.
- პლატფორმას ყოველდღიურად უნდა შეეძლოს ორგანიზაციის ძირითადი დომენის, ქვედომენებისა და დაკავშირებული დომენების მონიტორინგი, DNS ჩანაწერების (A, AAAA, NS, SPF, DMARC, MX) ცვლილებების შესახებ ელფოსტით/განგაშით შეტყობინებით.
- პლატფორმას უნდა შეეძლოს ორგანიზაციის DNS უსაფრთხოების შემოწმება და ისეთი არასწორი კონფიგურაციების იდენტიფიცირება, როგორიცაა SMTP Open Relay და Open Zone Transfer, შესაბამისი განგაშის გაგზავნით.
- პლატფორმას უნდა შეეძლოს აღმოჩენილი აქტივების გამჟღავნების რისკის ქულის ჩვენება სხვადასხვა მეტრიკის საფუძველზე — განგაშების რაოდენობა, დომენის ბაზისური ქულა, SSL პრობლემები, დაუცველობების რაოდენობა და სხვ.
- პლატფორმას ყოველდღიურად უნდა შეეძლოს ორგანიზაციის ძირითადი და დაკავშირებული დომენების WHOIS ჩანაწერების, ისტორიისა და ცვლილებების მონიტორინგი, ცვლილებების შესახებ ელფოსტით შეტყობინებით.
- პლატფორმას უნდა გააჩნდეს დეტალური აქტივის ინტელექტის ბარათები, რომლებიც აჩვენებს აღმოჩენის გზას, გეოგრაფიულ მდებარეობას, ინტერნეტში გამჟღავნებას, გაჟონვებსა და უსაფრთხოების დაუცველობებს თითოეული აქტივისთვის; ამ მონაცემებზე დაყრდნობით უნდა გამოითვლებოდეს რისკის ქულა და დგინდებოდეს გამოსწორების პრიორიტეტები.
- აღმოჩენილი/დამატებული დომენების, ქვედომენებისა და დაკავშირებული დომენების SSL სერტიფიკატები უნდა იმონიტორინგდებოდეს. დომენისა და SSL სერტიფიკატის ჩანაწერები და ისტორია უნდა იყოს ხელმისაწვდომი, ცვლილებებზე განგაშით; ასევე უნდა არსებობდეს მყისიერი SSL სკანირების შესაძლებლობა.
- პლატფორმას უნდა გააჩნდეს დეტალური შეფასების რეიტინგი SSL სერტიფიკატებისთვის კრიტიკული საკითხების პრიორიტეტიზაციისთვის და გამოვლენილი დაუცველობებისთვის განგაშის გენერირებისთვის.
- HTTP, TCP, UDP და ICMP სერვისები ყოველდღიურად უნდა მოწმდებოდეს. კრიტიკული პორტის განგაში უნდა იგზავნებოდეს, როდესაც ღიაა RDP, SSH, FTP, SMB SQL და NTP.

- პლატფორმას უნდა შეეძლოს აღმოჩენილი მობილური აპლიკაციებისთვის manifest XML გამონატანის მიწოდება, როგორც საბაზისო კონფიგურაციის კომპონენტისა.
- პლატფორმას უნდა შეეძლოს აღმოჩენილი აქტივების ტეგირება ან ლეიბლირება (მაგ.: „თანამშრომელი“) აქტივების პრიორიტეტიზაციისა და კონტექსტური გაგების გასაუმჯობესებლად.
- პლატფორმას უნდა შეეძლოს ქვედომენის ხელში ჩაგდების (Subdomain Takeover) შემოწმება და გამოვლენისას განგაშის გენერირება.
- პლატფორმას უნდა შეეძლოს ორგანიზაციის შეტყობინება, როდესაც გარეთ გამჟღავნებულ სისტემებში, ინფრასტრუქტურასა და ქსელურ აპლიკაციებში აღმოჩენილია ახალი დაუცველობა ან რისკი, როგორც აქტიური, ისე პასიური სკანირების საშუალებით.
- პლატფორმას უნდა შეეძლოს გამოვლენილი დაუცველობებისთვის CVSS-ის და საკუთარი დაფასტენების მეთოდის მიწოდება, ქულის დათვლის ლოგიკის განმარტებით.
- პლატფორმას უნდა შეეძლოს გამოვლენილი შეტევების ვექტორებისთვის გადაწყვეტის რეკომენდაციებისა და შერბილების ნაბიჯების მიწოდება, პოტენციურ თავდასხმებზე რეაგირების გზების აღწერით.
- პლატფორმას უნდა გააჩნდეს დაუცველობის მართვის სპეციალური გვერდი მარტივი გამოყენებისთვის, სორტირების ვარიანტებით სიმძიმის, სკანირების ტიპის, პროდუქტის დროისა და აღმოჩენის თარიღის მიხედვით, ასევე დაუცველობების დაჯგუფების ვარიანტით აქტივის ან CVE ID-ის მიხედვით.
- დაუცველობისა და რისკის შეტყობინებები მინიმუმ უნდა შეიცავდეს: აღმოჩენილი აქტივის ინფორმაციას, კრიტიკულობის დონეს, აღმოჩენის თარიღს, დაუცველობის ტიპსა და აღწერას, დაუცველობის ზეგავლენას, დეტალურ ინფორმაციას, ხელმისაწვდომ POC ინფორმაციას, გამოსწორებისა და შერბილების რეკომენდაციებს და წყაროებს.
- პლატფორმას უნდა შეეძლოს ახლად გამოვლენილი, ისევე როგორც ძველი დაუცველობების უწყვეტი მონიტორინგი 25 000-ზე მეტი მოდულის (plugin) გამოყენებით, რომლებიც ეფუძნება DoS, ვებაპლიკაციის ბოროტად გამოყენებას, უხეში ძალის შეტევებს, არასაჭირო სერვისებს და სხვ.
- პლატფორმას უნდა გააჩნდეს რეკომენდებული პოლიტიკები, რომლებიც შესაძლებელს ხდიან სპეციალურ სკანირებას გამომძალველი პროგრამების, OWASP Top 10, CISA KEV და ვებაპლიკაციის უსაფრთხოებასთან დაკავშირებული დაუცველობებისთვის.
- პლატფორმას უნდა შეეძლოს რეკომენდებული ან მორგებული პოლიტიკების გამოყენებით დაგეგმილი სკანირების ჩატარება მომხმარებლის მიერ არჩეულ დროს და ავტომატური შედეგების გენერირება უწყვეტი საფრთხის გამჟღავნების შეფასების (CTEM) ფარგლებში, სხვადასხვა სკანირების ლოკაციის არჩევის შესაძლებლობით რეალისტური თავდასხმის სიმულაციისთვის.
- პლატფორმას უნდა შეეძლოს მობილური აპლიკაციების გაფართოებული ანალიზი iOS აპ-სტორიდან IPA ფაილის ავტომატური ჩამოტვირთვით, ხელით ჩარევის გარეშე.

- პლატფორმას უნდა შეეძლოს ორგანიზაციის მობილურ აპლიკაციებში დაუცველობის ან უსაფრთხოების რისკის (მაგ.: ჩაშენებული საიდუმლო მონაცემები ან სუპერ-root პრივილეგიები) იდენტიფიცირება.

6. Unified Cyber Intelligence - Business License detailed breakdown:

- Company Name – 1
- Domain Limit - 3
- Brand Keyword – 75
- VIP account - 5
- User seats - 3
- Attack Surface Management
- Threat Search Credits - 1000
- Malware Analysis - 100
- Supply Chain Intelligence - 10
- Black Market Credit (\$) – 120
- Takedown as-a-service - 10
- Standard API Included
- Online Access to SOCRadar Academy

4. მონაწილეობის საკვალიფიკაციო მოთხოვნები

ტენდერში მონაწილეობის მისაღებად პრეტენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტაცია:

1. სამეწარმეო/საგადასახადო რეგისტრაციის დამადასტურებელი დოკუმენტი (ამონაწერი მეწარმეთა და არასამეწარმეო (არაკომერციული) იურიდიული პირების რეესტრიდან).
2. ამონაწერი, რომელიც ადასტურებს, რომ პრეტენდენტი არ იმყოფება ლიკვიდაციის ან გაკოტრების პროცესში.
3. ცნობა საგადასახადო დავალიანების არარსებობის შესახებ.
4. შესაბამისი გამოცდილების დამადასტურებელი დოკუმენტაცია (ბოლო 2 წლის განმავლობაში მინიმუმ 1 ანალოგიური ხელშეკრულების/მიწოდების დამადასტურებელი დოკუმენტი ან/და სარეკომენდაციო წერილი).
5. შეთავაზებული პროდუქციის ტექნიკური სპეციფიკაციები (მწარმოებლის დოკუმენტაცია/სპეც-ფურცელი).

6. შემოთავაზებული პროდუქციის მწარმოებელს (მოწყობილობების შემთხვევაში) საქართველოში უნდა ქონდეს ოფიციალური საგარანტიო მომსახურების სერვის ცენტრი.
7. ავტორიზაციის წერილი მწარმოებლისგან ან ოფიციალური დისტრიბუტორისგან.
8. ხელმოწერილი და ბეჭედდასმული სატენდერო წინადადება, ფასების ცხრილთან ერთად (დანართი №1).
9. პრეტენდენტს უნდა ჰყავდეს შესაბამისი ვენდორის სერტიფიცირებული ქართულ ენოვანი სპეციალისტი.
10. პრეტენდენტი არ უნდა იყოს საჯარო შესყიდვების - procurement.gov.ge შავ საშვი.
11. პრეტენდენტის მიერ შემოთავაზებული პროდუქტი არ უნდა იყოს შექმნილი/ნაწარმოებულია ქვეყნის უსაფრთხოებისთვის საფრთხის შემცველი ქვეყნის მიერ.
12. დამკვეთის ინფორმაციული ტექნოლოგიების გარემოში არსებულ მონაცემებზე დაშვების საჭიროების შემთხვევაში პრეტენდენტს უნდა ქონდეს დანერგილი ინფორმაციული უსაფრთხოების მართვის სისტემა და წარმოადგინოს შესაბამისი აუდიტის ანგარიში და კონტროლის მექანიზმების გამოყენებადობის განაცხადი (SOA).
13. პრეტენდენტის მიერ კონტრაქტორის გამოყენების საჭიროების შემთხვევაში აღნიშნული წინასწარ შემოთავაზების წარმოდგენისას უნდა აცნობოს დამკვეთს.

5. სატენდერო წინადადების წარდგენის წესი

სატენდერო წინადადება წარმოდგენილი უნდა იქნეს ელექტრონულად tenders.ge პლატფორმაზე.

დაგვიანებით წარმოდგენილი წინადადებები არ განიხილება.

6. სატენდერო წინადადებების შეფასების კრიტერიუმები

სატენდერო წინადადებები შეფასდება შემდეგი კრიტერიუმების მიხედვით:

შეფასების კრიტერიუმი
სატენდერო წინადადების ფასი
შეთავაზებული ტექნიკის მახასიათებლების შესაბამისობა/გადაჭარბება მინიმალურ მოთხოვნებთან
გარანტიის ვადა და საგარანტიო მომსახურების პირობები
მიწოდების ვადა

შემსყიდველი იტოვებს უფლებას, არ დააკმაყოფილოს არცერთი წარმოდგენილი წინადადება, საჭიროების შემთხვევაში მოითხოვოს დამატებითი ინფორმაცია/განმარტება პრეტენდენტისგან, ან შეწყვიტოს ტენდერის პროცედურა ნებისმიერ ეტაპზე.

7. ხელშეკრულების ძირითადი პირობები

- მიწოდების ვადა: ხელშეკრულების გაფორმებიდან 60 კალენდარულ დღეში.
- გადახდის პირობები: უნაღდო ანგარიშსწორება (საბანკო გადარიცხვა); ჯამური ღირებულების 40% წინასწარ ავანსის სახით, ხოლო დარჩენილი 60%, მიღება-ჩაბარების აქტის საფუძველზე, 10 კალენდარული დღეში.
- გარანტია: მოწოდებულმა პროდუქტმა უნდა უზრუნველყოს პროდუქტების ცხრილში (მუხლი 3) მითითებული მინიმალური საგარანტიო ვადები; მიმწოდებელი ვალდებულია უზრუნველყოს უფასო საგარანტიო მომსახურება/შეცვლა გარანტიის პერიოდში.
- პირგასამტეხლო: მიწოდების ვადის დარღვევის შემთხვევაში მიმწოდებელს დაეკისრება პირგასამტეხლო ყოველ ვადაგადაცილებულ დღეზე ხელშეკრულების ღირებულების 0.01% ოდენობით.
- შესყიდვა განხორციელდება საქართველოს კანონმდებლობის შესაბამისად.

8. დამატებითი პირობები

პრეტენდენტს უფლება აქვს, დასვას დამაზუსტებელი კითხვები წერილობით, ზემოთ მითითებულ საკონტაქტო ელ. ფოსტაზე, მუხლი 5-ში მითითებულ ვადამდე.

წინამდებარე დოკუმენტში ცვლილება/დამატება, საჭიროების შემთხვევაში, ეცნობება ყველა დაინტერესებულ პირს ტენდერის დასრულებამდე გონივრულ ვადაში.

ტენდერში მონაწილეობასთან დაკავშირებული ყველა ხარჯი ეკისრება პრეტენდენტს.

დანართი №1 — სატენდერო წინადადების ფასების ცხრილი

პრეტენდენტის დასახელება: [_____]

საიდენტიფიკაციო კოდი: [_____]

#	დასახელება	ერთეული	რაოდენობა	ერთეულის ფასი (დღგ-ს ჩათვლით)	ჯამური ღირებულება
1	Unified Cyber Intelligence • Company Name – 1 • Domain Limit - 3 • Brand Keyword – 75 • VIP account - 5 • User seats - 3 • Attack Surface Management • Threat Search Credits - 1000 • Malware Analysis - 100 • Supply Chain Intelligence - 10 • Black Market Credit (\$) – 120 • Takedown as-a-service - 10 • Standard API Included • Online Access to SOCRadar Academy	ცალი	1		
სულ ჯამური ღირებულება (დღგ-ს გარეშე):					

ფასები მითითებულია ლარში (GEL), დღგ-ს ჩათვლით.

პრეტენდენტის ხელმომწერი პირი: _____

თანამდებობა: _____

ხელმოწერა: _____ ბეჭედი: თარიღი: _____