## Cloud Sandboxing სისტემა

მოთხოვნები:

1. მოთხოვნილ Cloud Sandboxing სისტემას უნდა ქონდეს A და B ტიპის ბრანდმაუერებთან ინტეგრირების მხარდაჭერა.
2. მოთხოვნილ Cloud Sandboxing სისტემას უნდა მოყვებოდეს A ტიპის ბრანდმაუერისთვის Malware Protection 1 წლიანი ლიცენზია
3. მოთხოვნილ Cloud Sandboxing სისტემას უნდა მოყვებოდეს B ტიპის ბრანდმაუერისთვის Malware Protection 1 წლიანი ლიცენზია
4. მოთხოვნილ Cloud Sandboxing სისტემას უნდა მოყვებოდეს 1 წლიანი ლიცენზია არანაკლებ 3 (სამი) მომხმარებლის მხარდაჭერით.
5. მოთხოვნილ Cloud Sandboxing სისტემას უნდა გააჩნდეს ჩაშენებული არანაკლებ 200 ფაილი/დღე ატვირთვის საშუალება, დამატებითი ლიცენზიის გარეშე, A ან B ტიპის ბრანმაუერებზე Malware Protection ლიცენზიის შეძენის შემთხვევაში.
6. მოთხოვნილ Cloud Sandboxing სისტემას უნდა გააჩნდეს შემდეგი ტიპის ფუნქციონალი:
* უნდა გააჩნდეს ფაილების ანალიზის საშუალება ცნობილი ინფიცირებული ფაილების SHA256 ხეშების მიხედვით
* Malware ფაილების და მოვლენების ღრმა ანალიტიკის ფუნქციონალი
* არანაკლებ 1000 ტიპის Malware highly accurate საფთხეების ქცევითი ინდიკატორების მხარდაჭერა
* Malware საფრთხეების სტატიკური და დინამიური ანალიზის მხარდაჭერა
* ფაილების მანუალური ატვირთვის მხარდაჭერა
* Malware ფაილების ანალიზის და ქცევის დეტალური აღწერის და რეპორტინგის მხარდაჭერა
* შესაძლებელი უნდა იყოს შემდეგი რეპორტების მიღება: PCAP report, Process report, Artifact Report, File Activity Report, Network Activity Report.
* შესაძლებელი უნდა იყოს ინტერაქცია ინფიცირებულ ფაილებთან სისტემაში ჩაშენებული დაცული ვირტუალური ინფრასტრუქტურის საშუალებით (GloveBox)
* სისტემის მომხმარებლებს უნდა შეეძლოთ სხვა და სხვა ემულირებული ინფრასტრუქტურის არჩევა
* სისტემას უნდა გააჩნდეს ინფიცირებული ფაილების პრიორიტეტიზაციის მხარდაჭერა ჩაშენული ფუნქცოინალის მეშვეობით (Threat Score)
* სისტემას უნდა შეეძლოს რეტროსპექტიული მოვლენების გენერირება, რომელიც სისტემის მომხმარებელს დაეხმარება ქსელურ ინფრასტრუქტურაში ინფიცირებული ფაილების ლოკაციის დადგენაში
* SIEM და PROXY პროდუქტებთან ინტეგრაციის მხარდაჭერა
* (REST) API მხარდაჭერა
* სტანდარტული FEED ფორმატების მახრდაჭერა: JavaScript Object Notation (JSON), Structured Threat Information Expression (STIX) და CSV
1. მოთხოვნილ Cloud Sandboxing სისტემას უნდა გააჩნდეს შემდეგი ტიპის ფაილების ანალიზის მხარდაჭერა:
* .BAT - Batch files
* .CHM - Compiled HTML Help – Microsoft Compiled HTML Help
* .DLL - See: PE32 and PE32+
* .ISO - ISO image files
* .HTA - HTML Application
* .HWP, .HWT, .HWPX - Available on the win7-x64-kr VM only (specific to Hancom Office)
* .JAR - Java Archives
* .JS – JavaScript
* .JSE - Encoded JavaScript
* .JTD, .JTT, .JTDC, .JTTC: Available on the win7-x64-jp VM only (specific to Ichitaro)
* LNK - Windows shortcut files
* MSI - Microsoft Installer files
* MHTML - Mime HTML Files
* Microsoft Office Documents: .DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX
* PDF - Portable Document Format (detailed static forensics, including Javascript resources)
* PE32 Files and Executables (.EXE)
* Libraries (.DLL)
* .PE32+ files – Available on the win7-x64 VM only
* Executable (.EXE)
* .PS1 - Powershell
* .SWF - Flash Files
* URLs (As Internet Shortcut file, or submit the URL directly. Detailed static forensics or Javascript resources.)
* .VBE - Encoded Visual Basic
* .VBN - Virus Bin – See .ZIP
* .VBS - Visual Basic Script
* .WSF - Windows Script File
* .XML and XML Based Office Document Types (.DOCX, .XLSX, .PPTX)
* XML - Extensible Markup Language (.XML), An XML that is from Office will be opened in the corresponding program
* ZIP – Archive and Quarantine Formats, as well as .BZ2, .GZip, .XZ
* Quarantine file types including .SEP, .VBN

## დამატებითი მოთხოვნები

* მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (Manufacturers Authorization Form)