Specificația tehnică

H1	Hardware – Cerințe Generale
H1.01.	Soluția propusă trebuie să fie livrată, instalată și configurată pentru a obține o soluție complet funcțională la cheie.
H1.02.	Toate componentele hardware a soluției trebuie să fie rack-mount 19”
H1.03.	Toate componentele hardware a soluției trebuie să fie compatibile cu rețeaua de curent electric AC120/230V 50/60Hz
H1.04.	Toate componentele hardware a soluției trebuie să aibă blocuri de alimentare interne redundante
H1.05.	Toate componentele hardware a soluției trebuie să fie funcționale la temperaturi de la 0°C până la 40°C
H1.06.	Soluția propusă trebuie să fie livrată cu toate cablurile necesare pentru conectare în rack C14 0,5m
H1.07.	Soluția propusă trebuie să aibă suport hardware și software pentru cel puțin 3 ani
H1.08.	Soluția propusă trebuie să aibă toate subscripțiile necesare active cel puțin 3 ani
H1.09.	Echipamentul hardware trebuie să asigure air-flow front-to-back

H2	Hardware – Cerințe funcționale
H2.01.	Soluția propusă este destinată centrelor SOC pentru monitorizarea și analiza evenimentelor de securitate
H2.02.	Soluția propusă trebuie să poată funcționa în doua regimuri: colectare sau analiză
H2.03.	Soluția propusă trebuie să poată fi gestionată dintr-o consolă centralizată web, ssh
H2.04.	Soluția propusă trebuie să genereze rapoarte conform șabloanelor prestabilite sau personalizate cu notificări automate pe e-mail în formate PDF, HTML, CSV și XML
H2.05.	Soluția propusă trebuie să permită generarea rapoartelor programate
H2.06.	Soluția propusă trebuie să permită personalizarea paginii de titlu a rapoartelor
H2.07.	Soluția propusă trebuie să permită crearea șabloanelor de rapoarte proprii

H2.08.	Soluția propusă trebuie să permită exportarea evenimentelor în format CSV sau Text, cu posibilitatea de compresare în format gzip
H2.09.	Soluția propusă trebuie să permită vizualizarea calendaristică a rapoartelor generate
H2.10.	Soluția propusă trebuie să permită vizualizarea în timp real a atacurilor
H2.11.	Soluția propusă trebuie să permită utilizarea mai multor instanțe virtuale cu alocarea spațiului pentru fiecare instanță
H2.12.	Soluția propusă trebuie să permită funcționarea atât în mod standalone cât și în HA
H2.13.	Soluția propusă trebuie să colecteze evenimente de securitate compatibil cu echipamentele fizice instalate de tip NextGenerationFirewall Fortinet și alte echipamente ce transmit Syslog mesaje
H2.14.	Soluția propusă trebuie să permită configurarea per fiecare instanță virtuală perioada de retenția evenimentelor pentru analiză și perioada de arhivare
H2.15.	Soluția propusă trebuie să suporte dashboard-uri cu vizualizarea grafică a atacurilor în timp real, sumarul după tipul atacului, IP-uri sursă și destinație
H2.16.	Soluția propusă trebuie să permită gestionarea conturilor de administrator cu filtrarea drepturilor de vizualizare
H2.17.	Soluția propusă trebuie să permită autentificarea utilizatorilor prin diferite tipuri de autentificare: local, radius, tacacs
H2.18.	Soluția propusă trebuie să suporte cel puțin 2000 de instanțe virtuale
H2.19.	Soluția propusă trebuie să aibă capacitatea de a analiza cel puțin 60000 logs/sec
H2.20.	Soluția propusă trebuie să aibă capacitatea de colectare a cel puțin 3000 GB loguri pe zi
H2.21.	Soluția propusă trebuie să aibă capacitate de stocare de cel puțin 40TB
H2.22.	Soluția propusă trebuie să susțină hardware RAID 0/1/5/6/10/50/60
H2.23.	Soluția propusă trebuie să suporte hotswap HDD
H2.24.	Soluția propusă trebuie să conțină cel puțin 4 porturi 1xGE RJ45
H2.25.	Soluția propusă trebuie să conțină cel puțin 2 porturi 10xGE SFP+
H2.26.	Fiecare echipament hardware trebuie să conțină cel puțin 1 RJ45 Console Port