Аңдатпа

SYSTEM (information and security event management technology) технологиясын пайдалану ақпараттық қауіпсіздік саласындағы, әсіресе сыни инфрақұрылымдар үшін перспективалы бағыт болып табылады. Дипломдық жобаның тақырыбы - " FortiSIEM "қолдану арқылы қауіпсіздікті және өнімділікті басқарудың кешенді, масштабты құралы". SIEM жүйесі жүйеде болып жатқан ең толық суретті алуға мүмкіндік береді. Бұл сондай-ақ IB оқиғалары туралы егжей-тегжейлі есептерді жасауға және оларға жылдам жауап беруге мүмкіндік береді.

SIEM жүйесіне кіруге рұқсат етілмеген әрекет жасалды. Инциденттің ауқымды шешімін қамтамасыз ету үшін Debian базасында VPN-сервері пайдаланылды, яғни қорғалған VPN-қосылым арқылы әр аймақтан қызметкерлерді тарту.

Ауа баптау және өрт қауіпсіздігі жүйелерін есептеумен еңбек жағдайларына талдау жүргізілді.