

Нет.Лог е Систем за управување со сигурносни информации и настани кој во себе обединува повеќе од 17 јавно достапни и лицензни сигурносни програми кои овозможуваат покривање на целокупното подрачје на управувањето со сигурноста на повеќе различни технолошки нивоа.

Нет.Лог е една од компонентите од програмата на **Нет.Бит** за обезбедување на информативна сигурност на организациите.

Нет.Лог во себе ги содржи сите современи механизми за контрола и справување со сигурносните ризици.

Нет.Лог е дизајниран и развиен така, што и покрај високото ниво на функционалност, обезбедува големи заштеди за организациите: голем дел од софтверот е бесплатен (open source), работи на платформа Linux/MySQL која исто така е бесплатна.

Нет.Лог е компатибилен со голем број производи и околина. Инженерите на **Нет.Бит** го имплементираат **Нет.Лог** по принципот клуч-на-рака, соодветно на потребите и инфраструктурата на организацијата.

Нет.Лог

Нет.Лог е комплексен и моќен систем кој има капацитет да обедини сигурносни програми и мрежни контролори за:

- Систем за детекција на неовлстени упади (IDS)
- Скенер на ранливости на системите
- Мониторинг на мрежите
- Следење на достапноста на ресурсите
- Детектори на аномалии
- Пасивни монитори
- Мрежни скенери
- Детална анализа и вештачење
- База на ранливости, и др.

Освен овие продукти, постојат и наменски развиени дополнителни модули кои се исто така вклучени заедно со претходните во **Нет.Лог** решението:

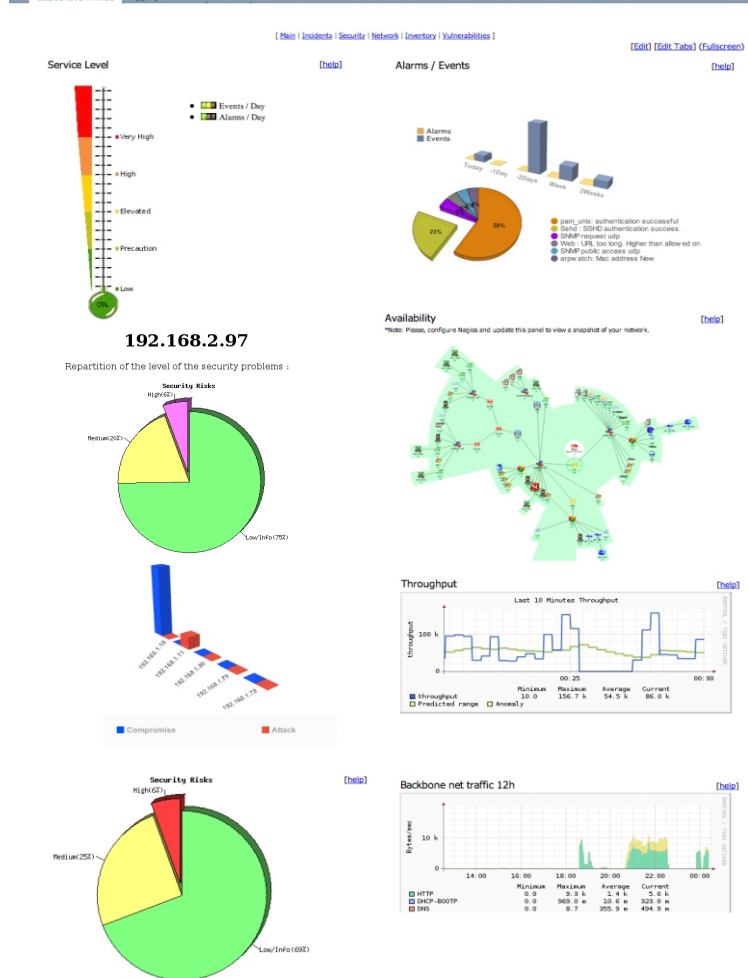
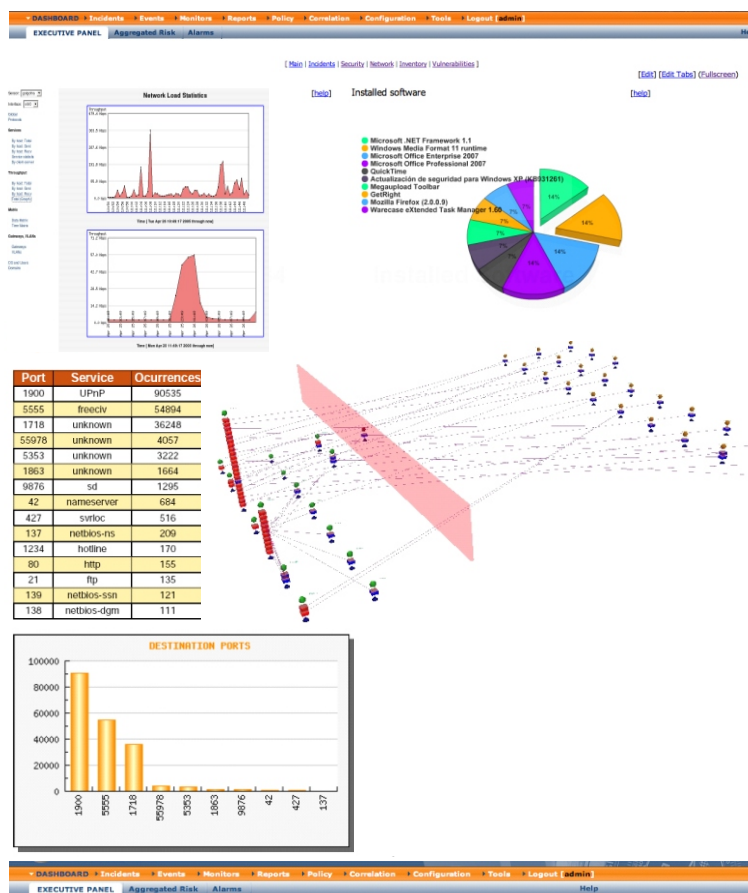
- Колекторски систем
- Корелатор на настани
- Инвентарен менаџер
- Управување со политиката на прибирање на настани
- Сигурносни и регулаторни извештаи
- Управување со инциденти и одговори
- Сигурносна усогласеност и рангирање на ризици

Нет.Лог претставува првенствено интегрирачки предизвик. Целокупниот развој се базира на интеграцијата на погоре споменатите софтвери. За таа цел е развиена корелациона техника и неколку алатки за извештаи и управување кои овозможуваат прибирање, нормализација и обработка на информациите преку една конзола.

Вака обединетите алатки овозможуваат тесна контрола на големи мрежи преку разместување на ниско-буџетни сензори и управување на информациите од една централна точка.

Нет.Лог е перформантен систем кој овозможува примена во развиени мрежи со голем број сензори во телекомуникациски, финансиски и владини организации и институции.

Net.Log



Нет.Лог нуди голем број на функционалности кои помагаат и го олеснуваат управувањето со сигурноста како што се:

- Апстракција
- Филтрирање на лажни тревоги
- Управување со ризици
- Автоматски одговори
- Следење на текови
- Управување со инциденти
- Сигурносни извештаи и судска експертиза

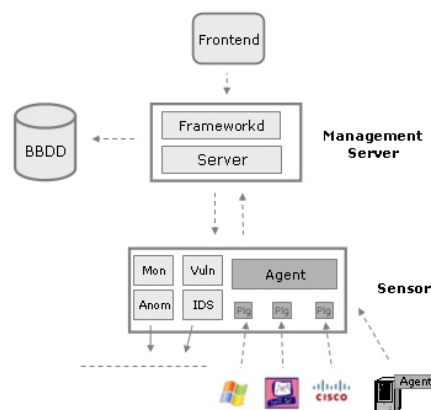
Визуелизација

Нет.Лог дава одличен преглед и визуелизација на надгледуваните системи, вклучувајќи детален и повеќе-нивовски мониторинг, како и генерирање на соодветни безбедносни аларми.

Архитектура

Типичната **Нет.Лог** инсталација се состои од 4 елементи како што е прикажано на сликата:

1. Сензори (Агенти)
2. Менаџмент сервер
3. База на податоци (Database)
4. Конзола – кориснички интерфејс (Frontend)



Нет.Лог може да прифаќа настани од други комерцијални уреди или прилагодени апликации благодарение на специфични и општи конфигурабилни додатоци (плаг-инови). Со тоа овозможува компатибилност и вклучување и на други безбедносни апликации во една функционална целина.

