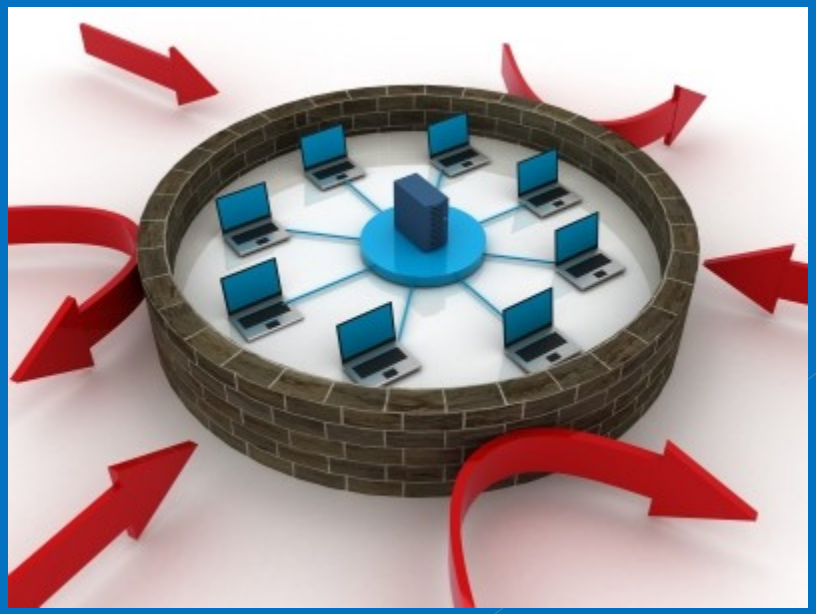
ВИКОРИСТАННЯ ВІЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ ТА СИСТЕМ

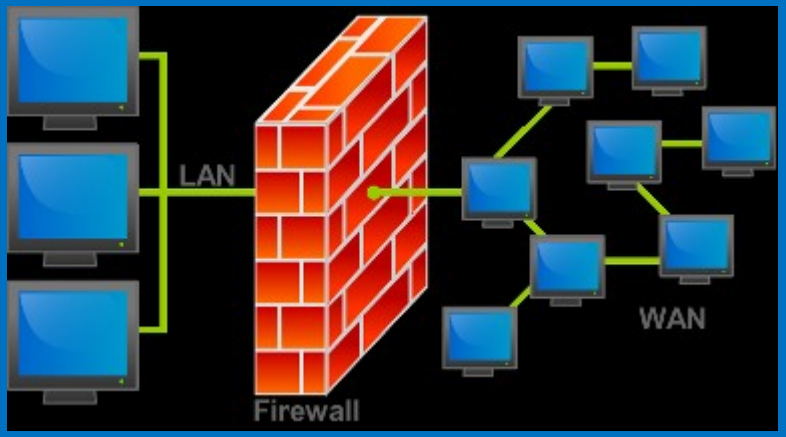
Національний університет Львівська політехніка

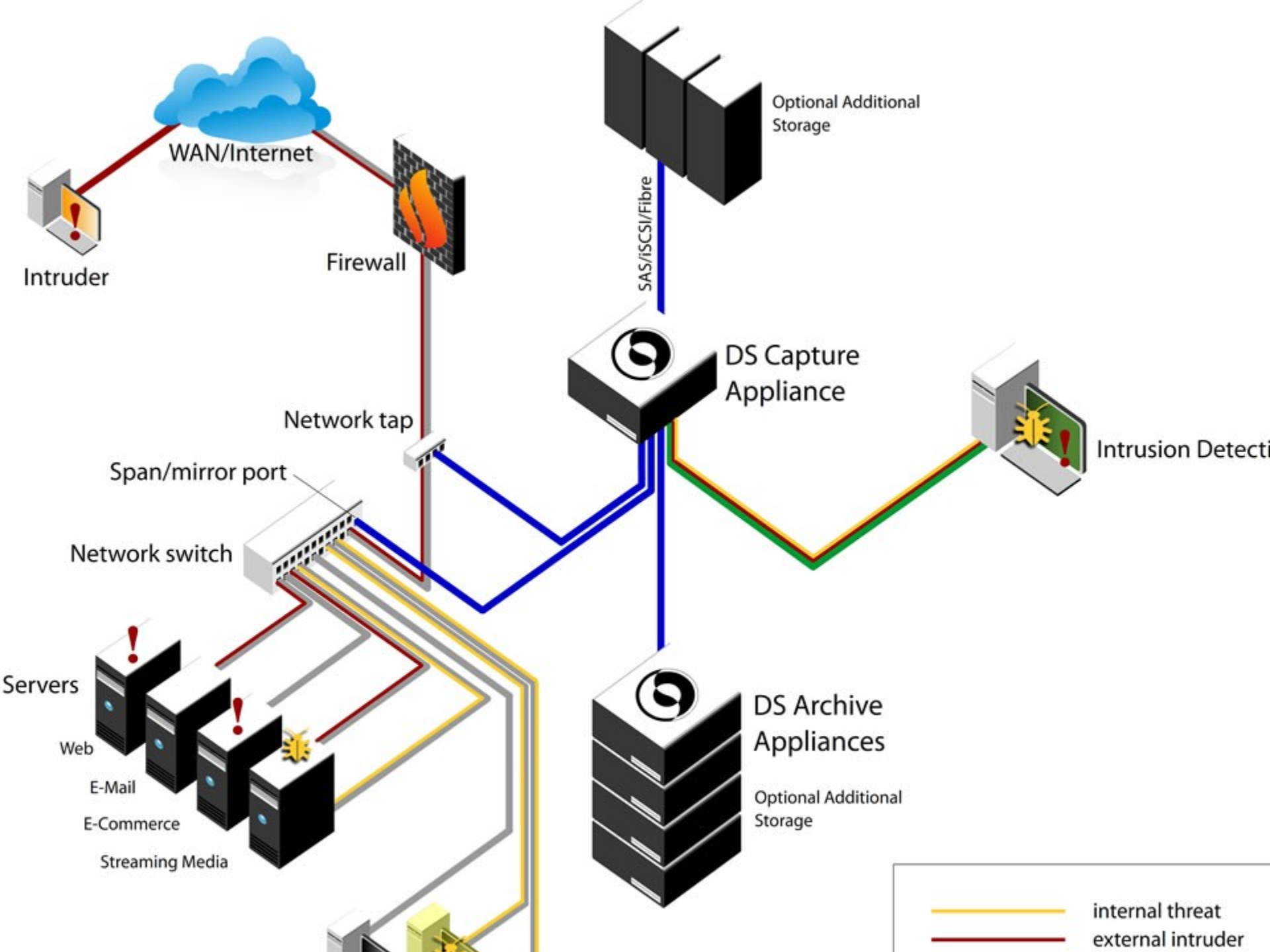
Андріян Піскозуб, 2012

- Чи безпека інформації актуальна?
- Що розуміють під безпекою інформації

Міжмережеві екрани

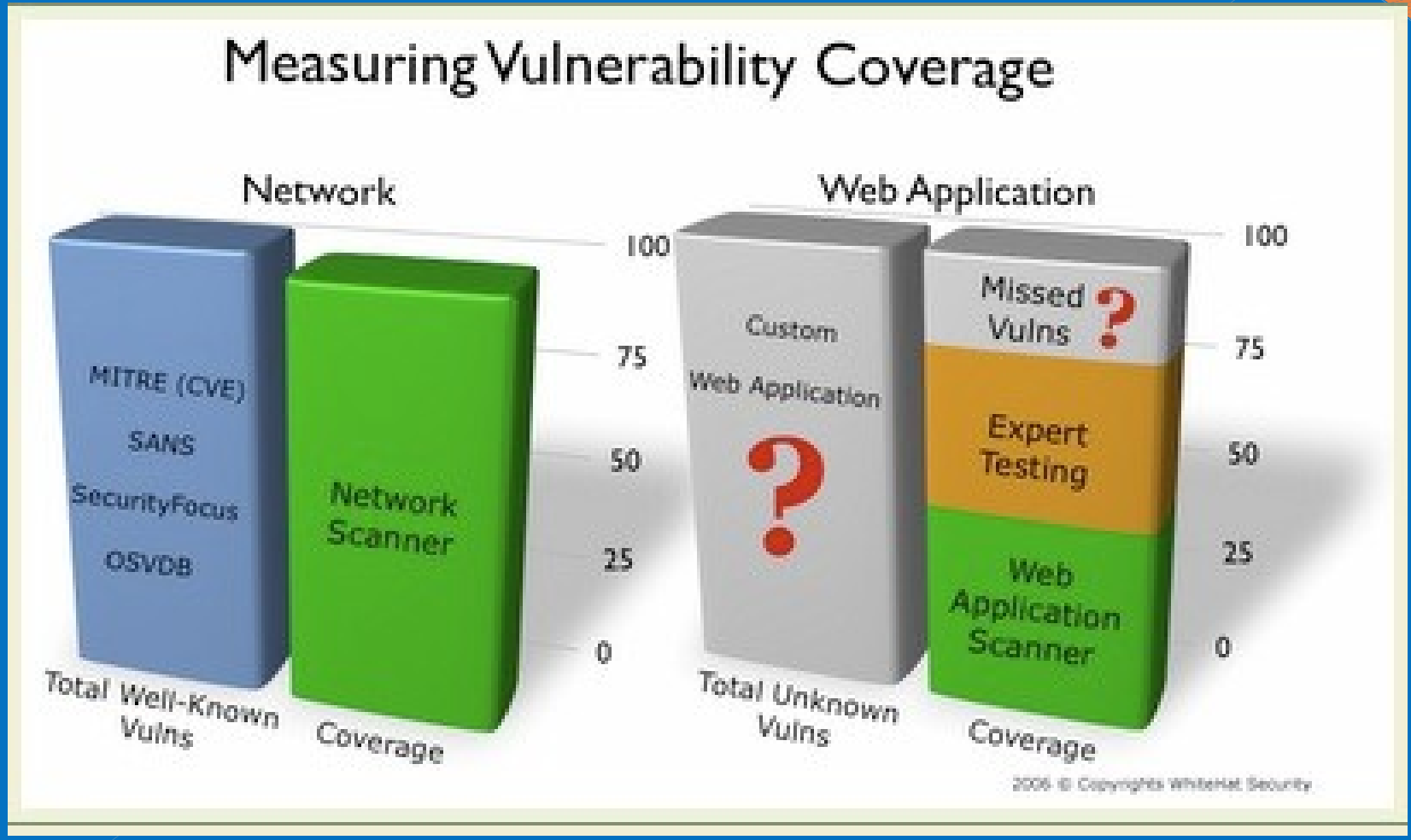





WAN/Internet
Intruder
Firewall
Optional Additional Storage
SAS/iSCSI/Fibre
DS Capture Appliance
Network tap
Span/mirror port
Network switch
Intrusion Detecti
Servers
Web
E-Mail
E-Commerce
Streaming Media
DS Archive Appliances
Optional Additional Storage
internal threat
external intruder

- Список інструментів підвищення рівня захищеності :
- сканери вразливостей
- системи тестування на проникнення
- системи журналізації подій

- сканери вразливостей



- Список інструментів підвищення рівня захищеності :
- сканери вразливостей
- системи тестування на проникнення

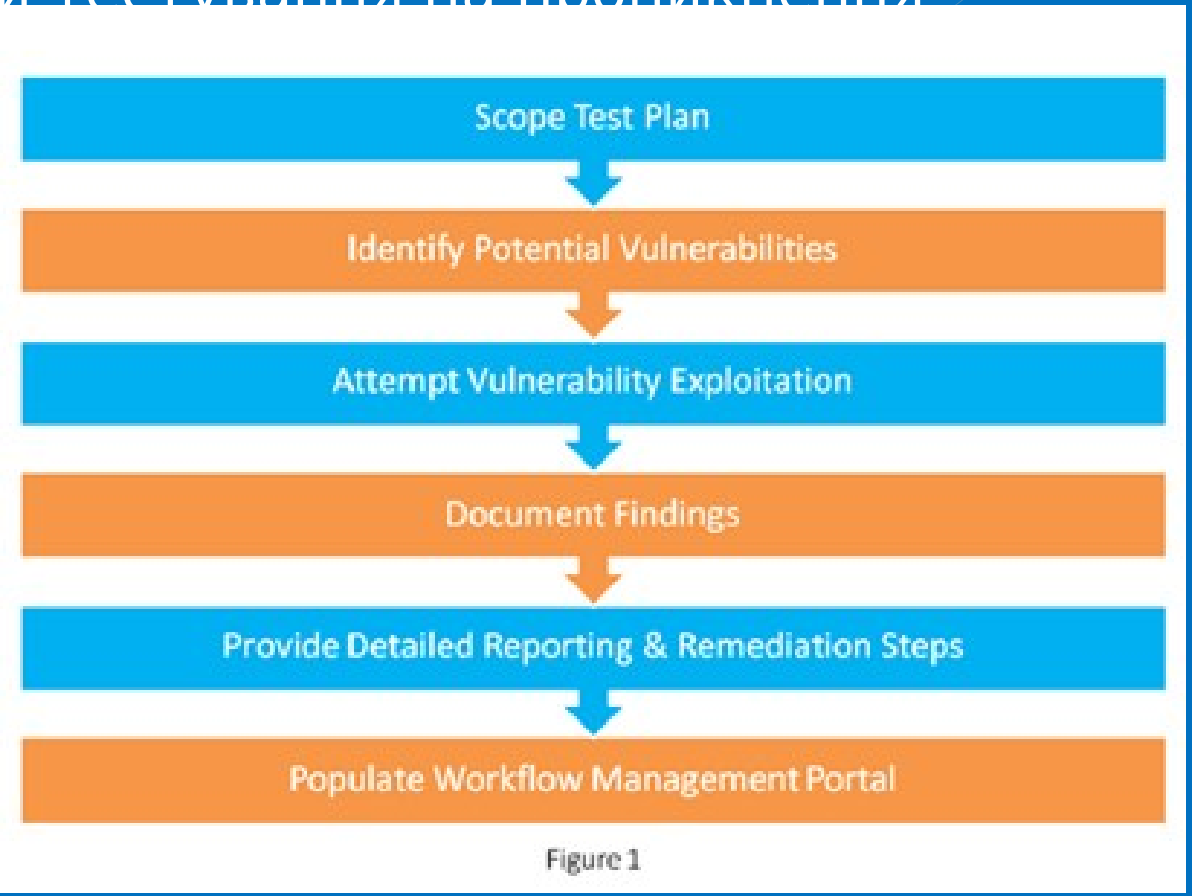
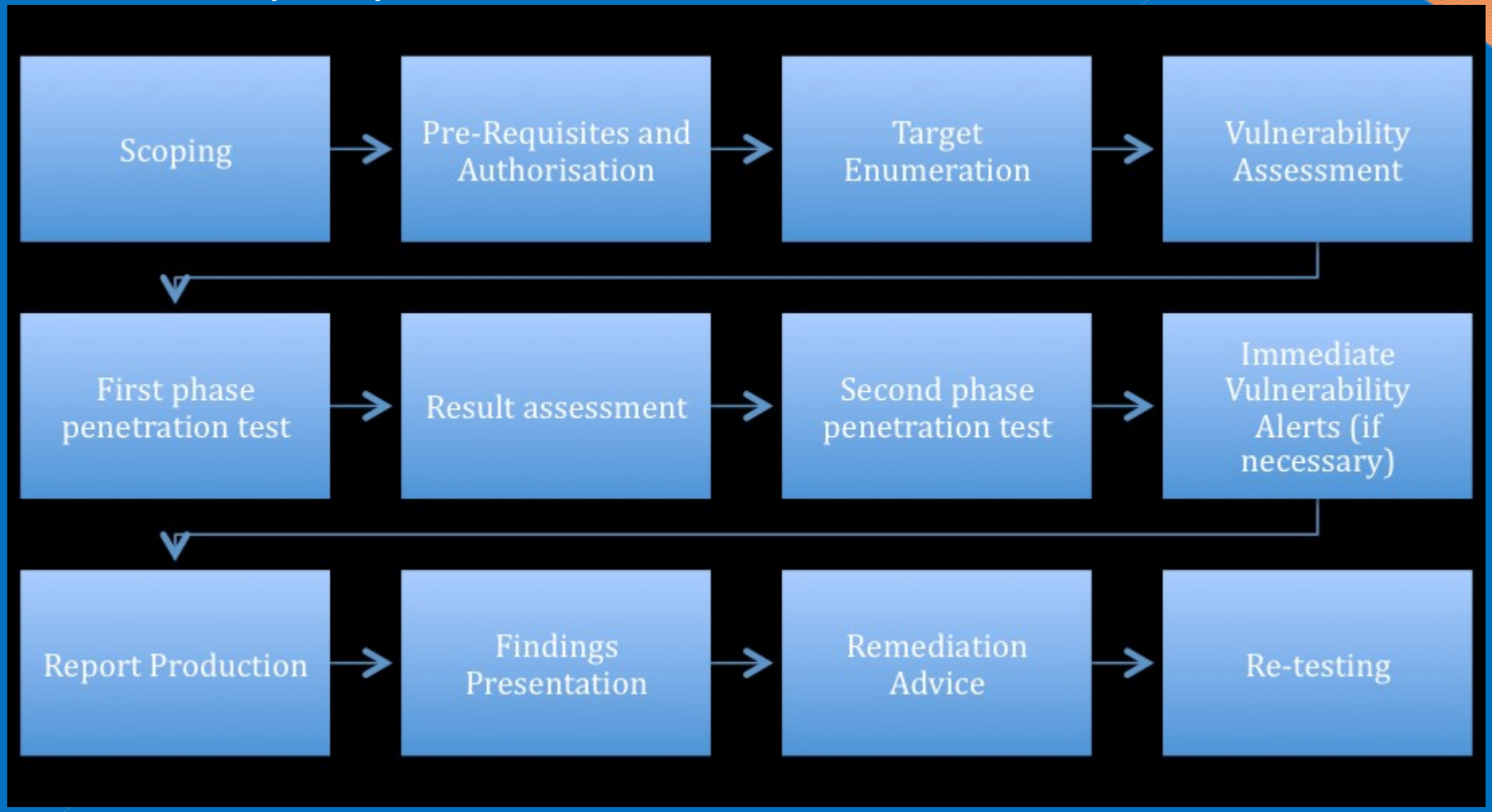
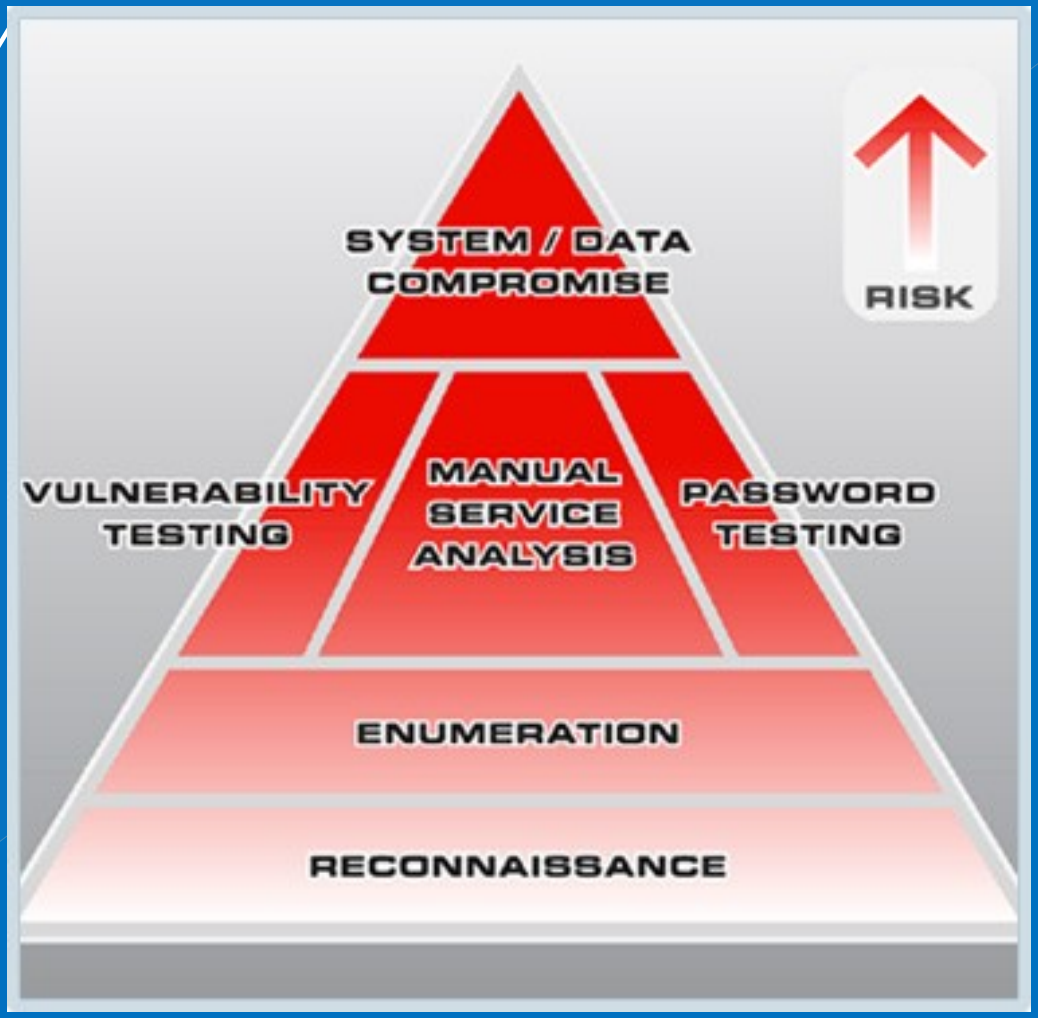


Figure 1

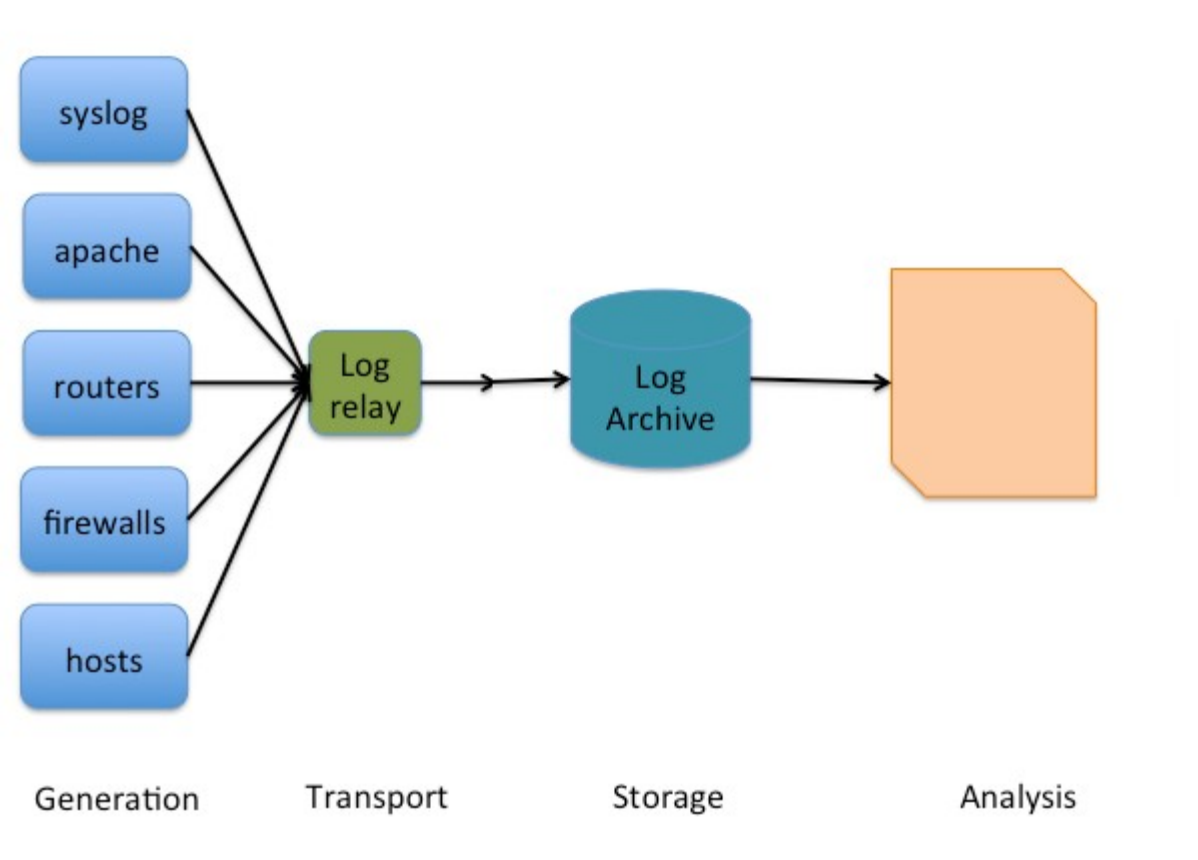
- Список інструментів підвищення рівня захищеності :
- сканери вразливостей



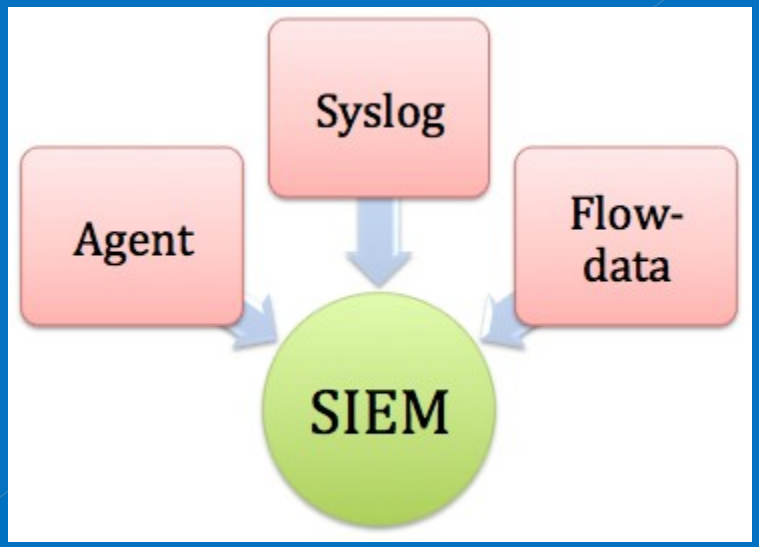
- Список інструментів підвищення рівня захищеності :
- системи



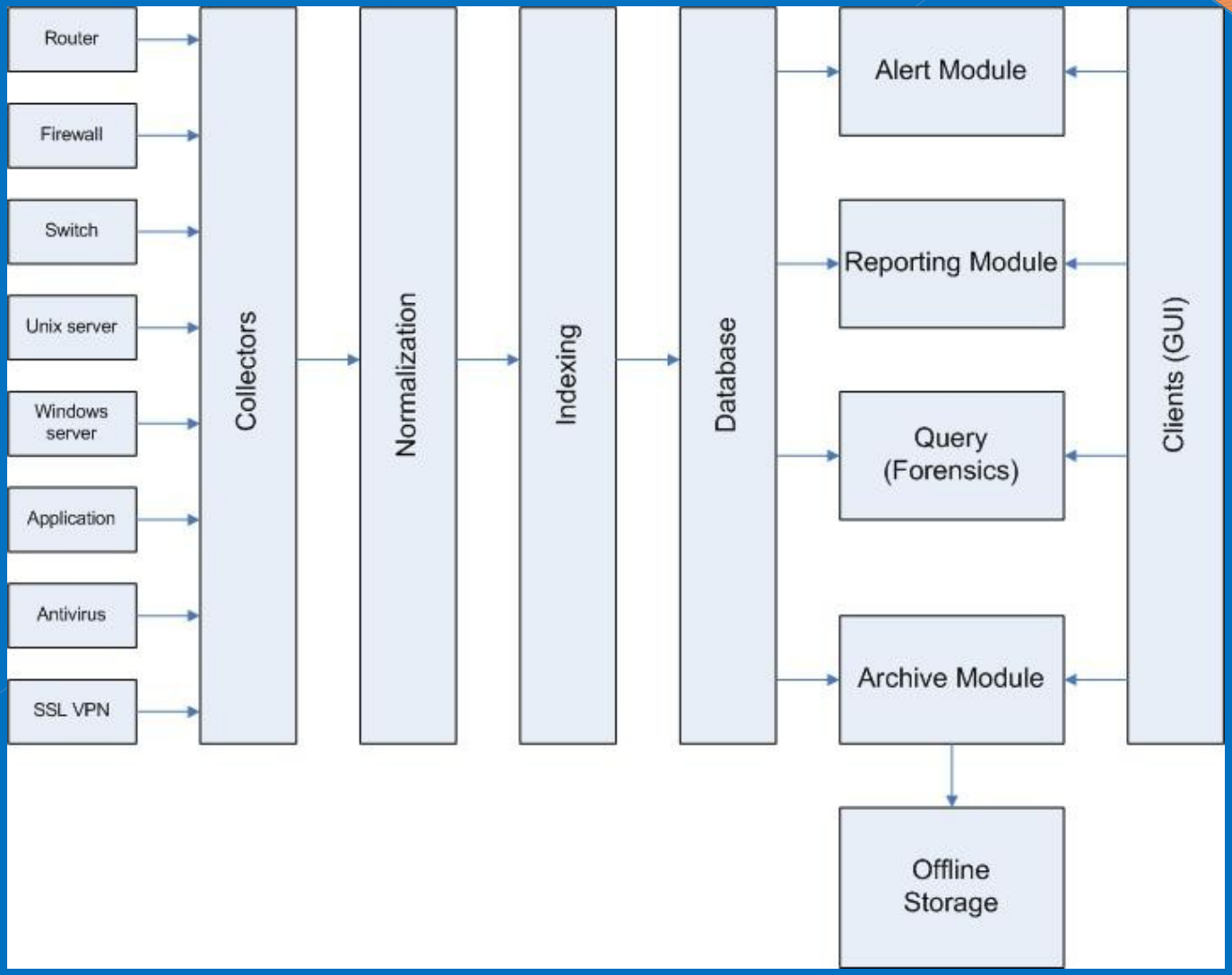
- Системи журналізації подій - чи достатньо просто зберігати журнали?
- Як їх опрацьовувати?



- Системи журналізації подій - чи достатньо просто зберігати журнали?
- Як їх опрацьовувати?



- системи управління інформацією та повідомленнями безпеки (Security Information and Event Management (SIEM)



https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management

OSSIM

Sponsors shown in green

Log Management & Security Information and Event Management (SIEM) 85

Request Information from Vendors

Select Up to 5 Products to Compare

PRODUCT INFO | RESOURCES | AWARDS | CERTIFICATIONS & COMPLIANCE

	Product	Vendor	Description	License
	RECENTLY UPDATED			
☐	Counter Tack	CounterTack	Improve your intelligence and incident response capabilities. CounterTack provides organizations with broader and richer, site-specific intelligence,...	Commercial
☐	EventSentry	NETIKUS.NET ltd	EventSentry is an affordable yet flexible real-time log, system and network monitoring suite. You can receive event log alerts through a variety of...	Commercial
☐	NetWrix Event Log Manager	NetWrix Corporation	Event log data is a unique source of information for security, audit, compliance and troubleshooting. Native event logging mechanisms provided by...	Freeware
☐	CorreLog Solution Suite	CorreLog	CorreLog, Inc. offers log management, unique security event correlation, and high-speed indexed search services. Our pure-software solutions enhance...	Commercial
☐	LogRhythm High Availability Solutions	LogRhythm	Maximum Uptime for Enterprise Information Assurance. With a powerful, high-performance, and feature-rich enterprise console, LogRhythm provides IT...	Commercial
☐	LogRhythm Host Activity Monitoring	LogRhythm	Protecting your organization from advanced threats, compliance violations and operational issues is an ongoing process. It requires broad visibility,...	Commercial
☐	LogRhythm Log & Event Management	LogRhythm	Historically, log management and event management have been viewed by most as two distinct functions that operated independently, and were usually...	Commercial
☐	LogRhythm Log Management & SIEM 2.0	LogRhythm	LogRhythm is an enterprise-class platform that seamlessly combines Log Management & SIEM 2.0, File Integrity Monitoring, and Host Activity Monitoring...	Commercial
☐	Akab	Araknos	Akab is a modular and scalable SIEM+ (Security Information Event Management) architecture composed of various appliances placed on different points of...	Commercial
☐	AlienVault Open Source SIEM (OSSIM)	AlienVault	AlienVault Open Source SIEM (OSSIM) is a complete Security Management solution available at no cost. Along with the AlienVault Unified SIEM, AlienVault...	Open Source

Кінцева реалізація

- Вибір ОС – простий чи ні ?
- Апаратне забезпечення - Intel Core i5, 8GB, 500 Gb HDD ?

- 3 віртуальні хости на базі VMWare ESXi 5:
- – системи централізованого збору та обробки інформації журналів подій (ОС Linux CentOS 6.2)
- – системи оцінки вразливостей та тестування на втручання (Back Track 5 на базі ОС Linux Ubuntu 10.04)
- – системи управління інформацією та повідомленнями безпеки (OSSIM на базі ОС Linux Debian 6)

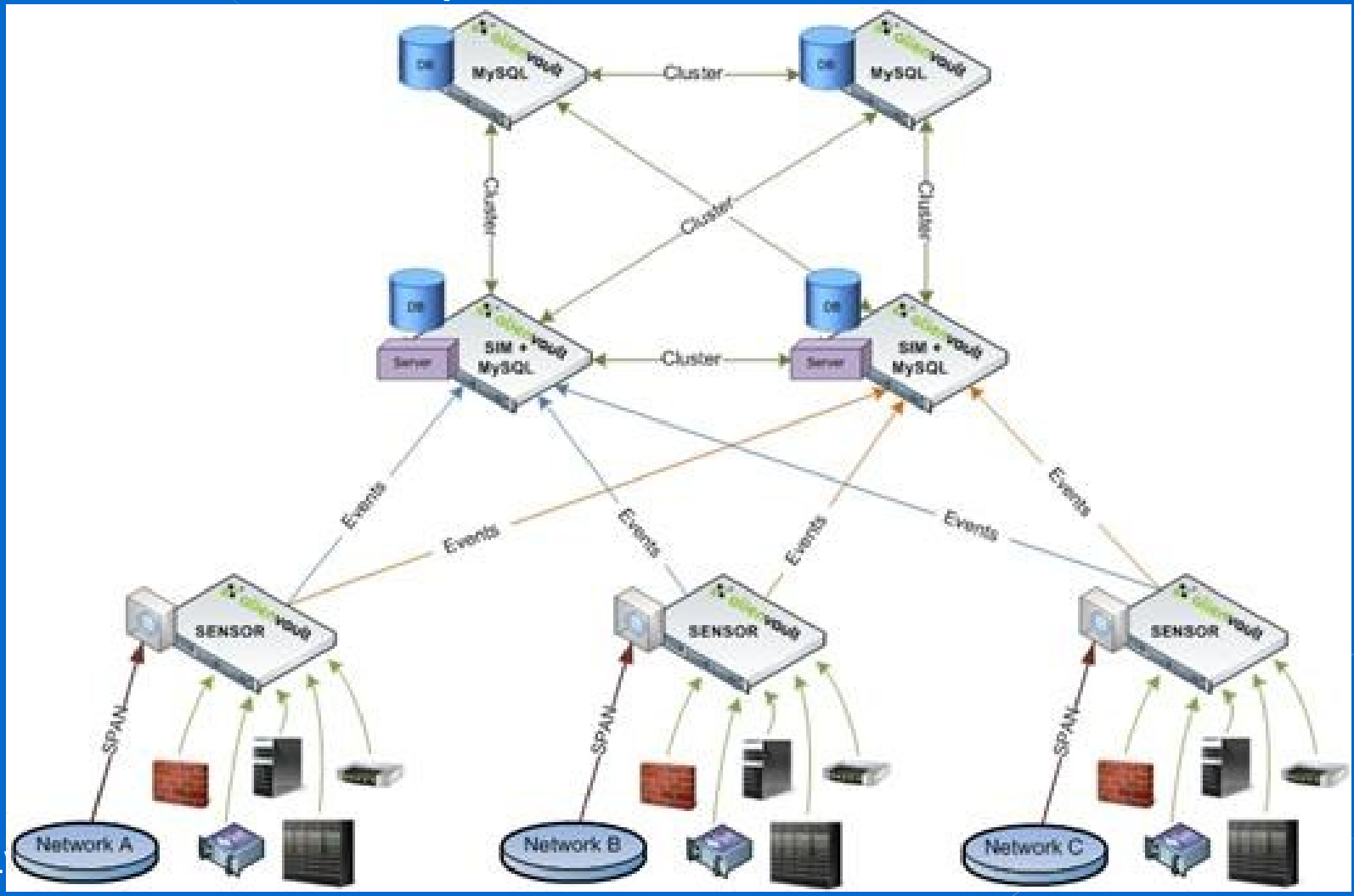
Система централізованого збору та обробки інформації журналів подій (ОС Linux CentOS 6.2)

- iptables,
- системи журналізації syslog-подій у складі rsyslogd, loganalyzer, Snare, Sagan, Snort

Система оцінки вразливостей та тестування на втручання (Back Track 5 на базі ОС Linux Ubuntu 10.04)

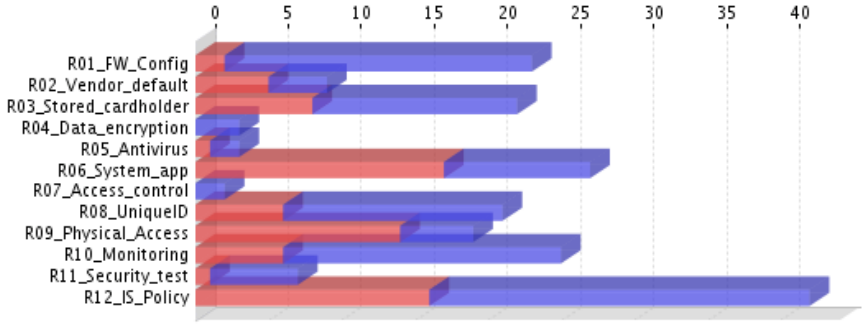
- iptables,
- tcpdump, wireshark;
- nmap;
- openvas, Nexpose Community edition, w3af, wapiti, nikto, arachni;
- Metasloit Framework, Metasploit Community edition

Система управління інформацією та повідомленнями безпеки (OSSIM на базі ОС Linux Debian 6)

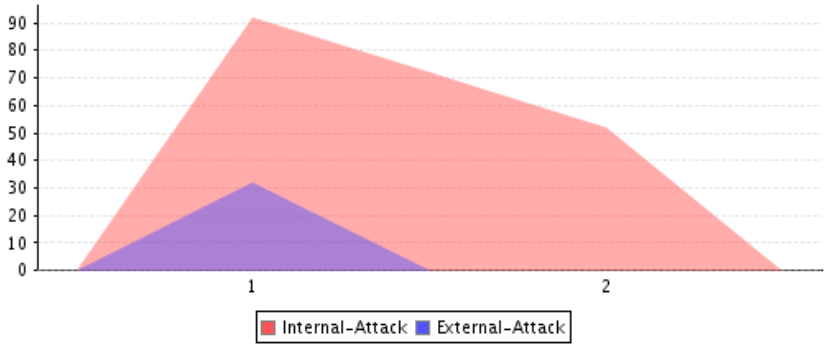


Dashboards
Dashboards
Risk
Incidents
Analysis
Reports
Assets
Intelligence
Monitors
Configuration
Tools
Logout [admin]
Maximize

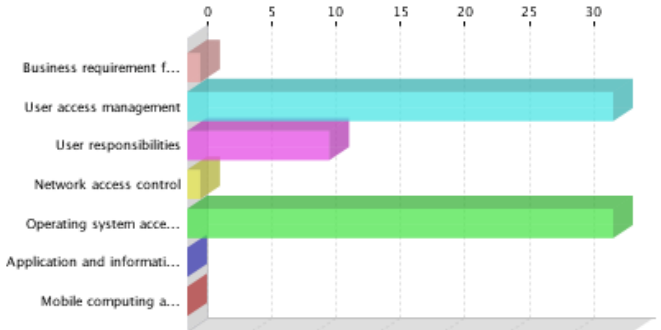
PCI-DSS - Self Assessment Questionnaire

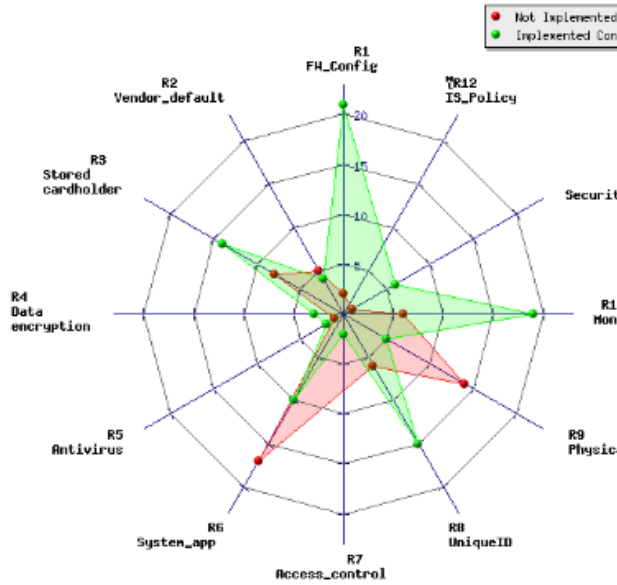


Trends Internal vs External threat by Month



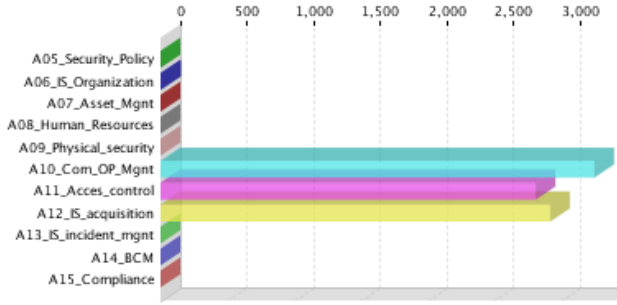
ISO27001 - Details - A11 Access Control





PCI-DSS - Details - R5 Antivirus

ISO27002 - Potential impacts - risks



PCI-DSS - Potential impacts

ПИТАННЯ?

ДЯКУЮ ЗА УВАГУ!

azpiskozub@gmail.com