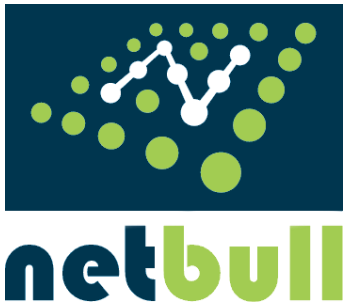
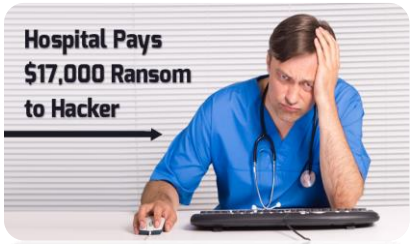
# Ανεικονικές Απειλές και Τρόποι Αντιμετώπισης




30/03/2017 | **Nikitas Kladakis**
**Information Security Director**

# Ανεικονικές Απειλές

**Απειλές οι οποίες δεν είναι ορατές και δεν έχουμε σχηματισμένη εικόνα**

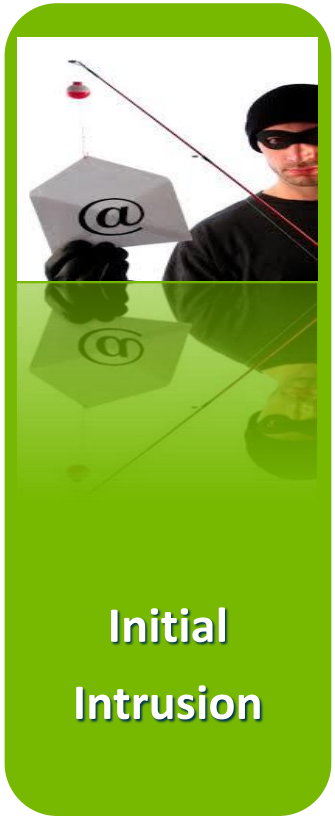


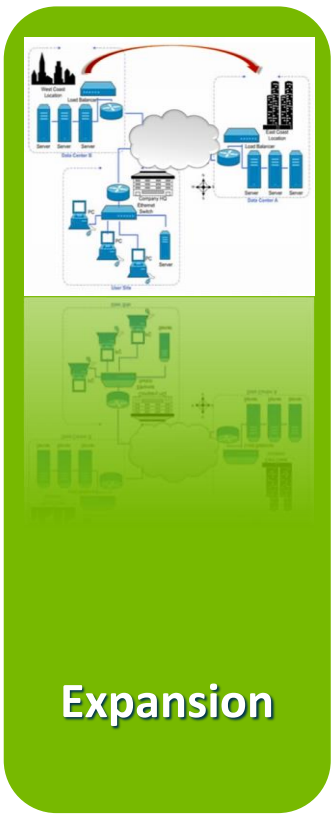


# Τα χαρακτηριστικά τους


1. Attack Methodology
2. Exploit using a zero day vulnerability
3. What you are seeing …
4. What is actual there …

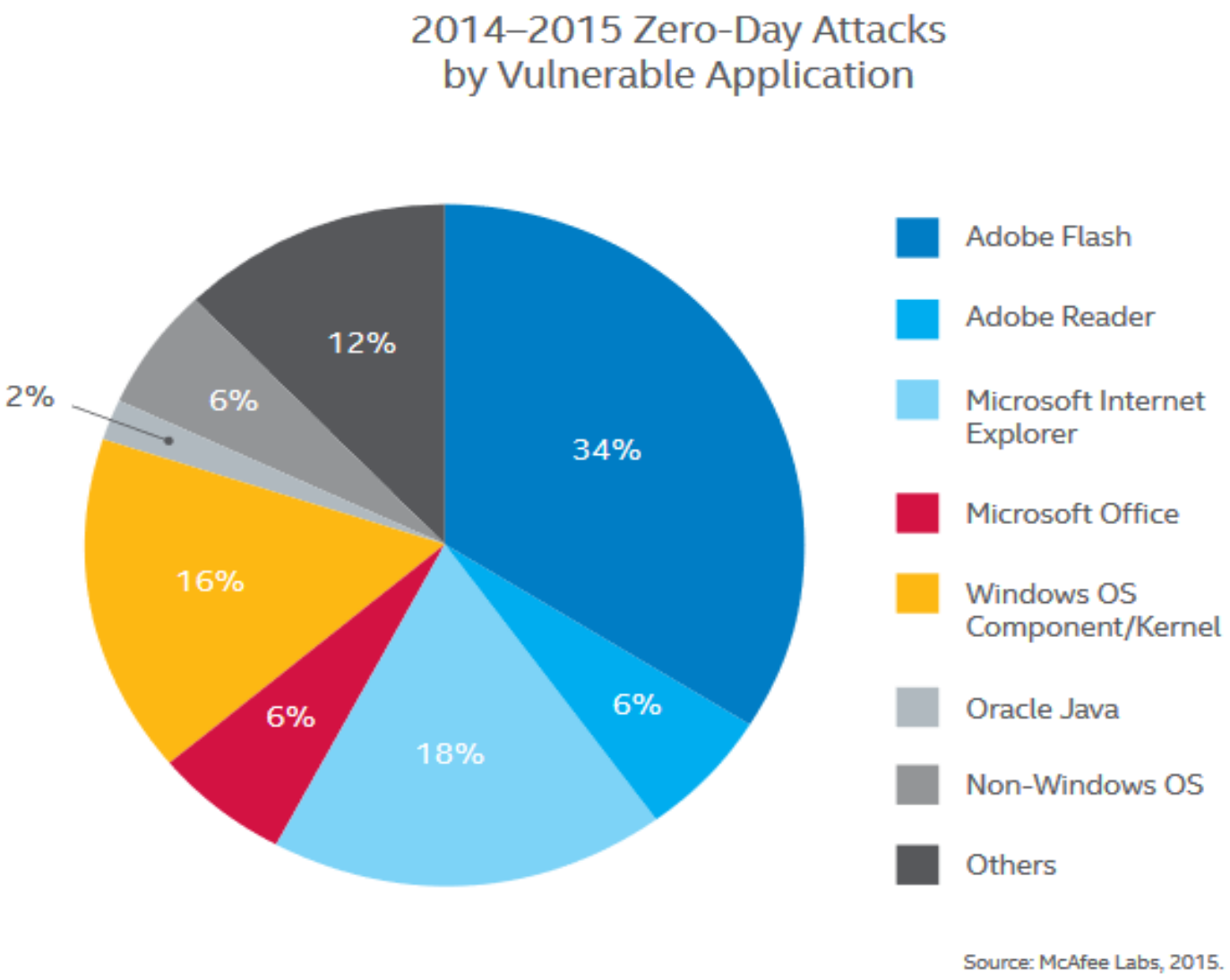
# Attack Methodology

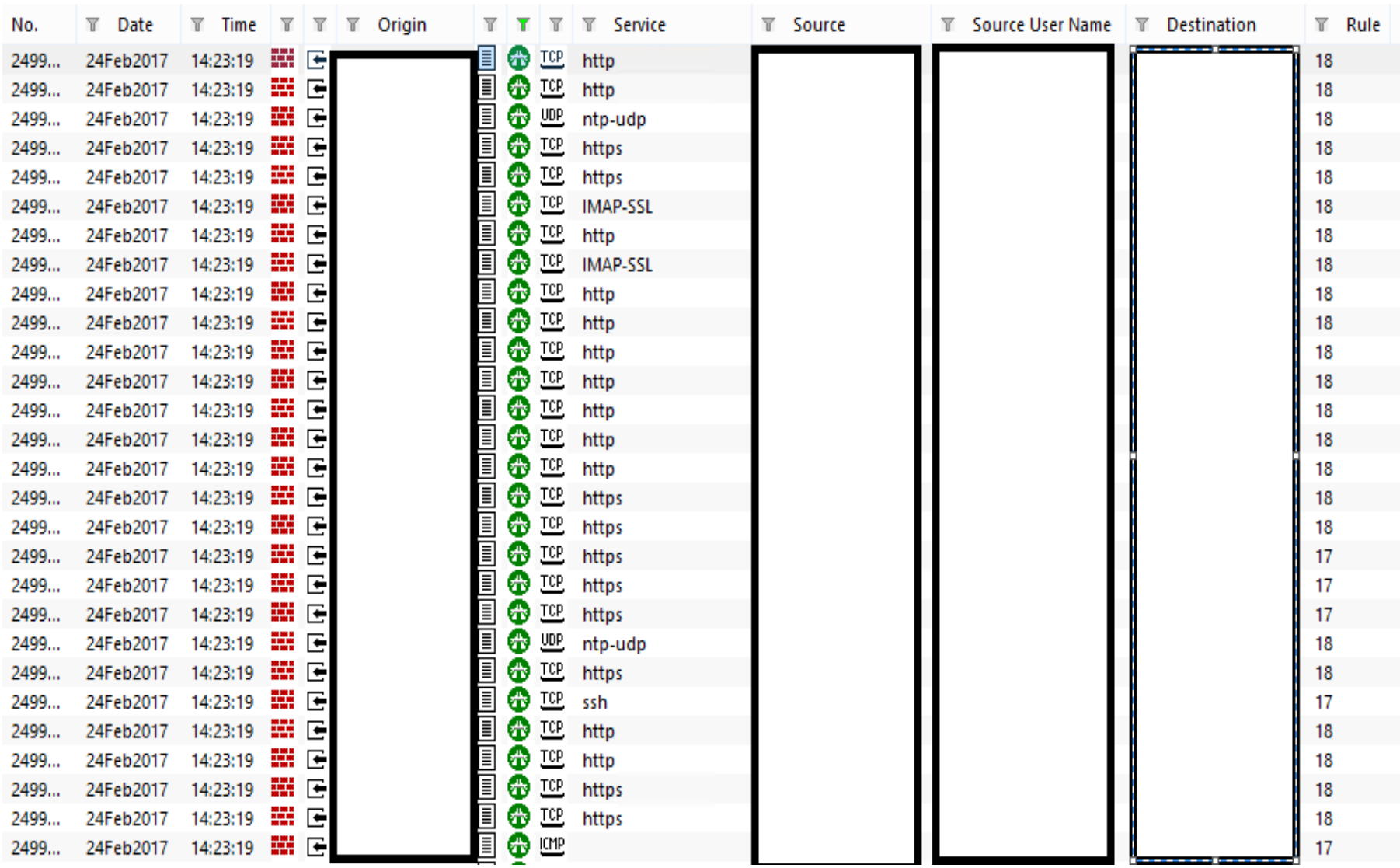


# Zero Day Vulnerabilities



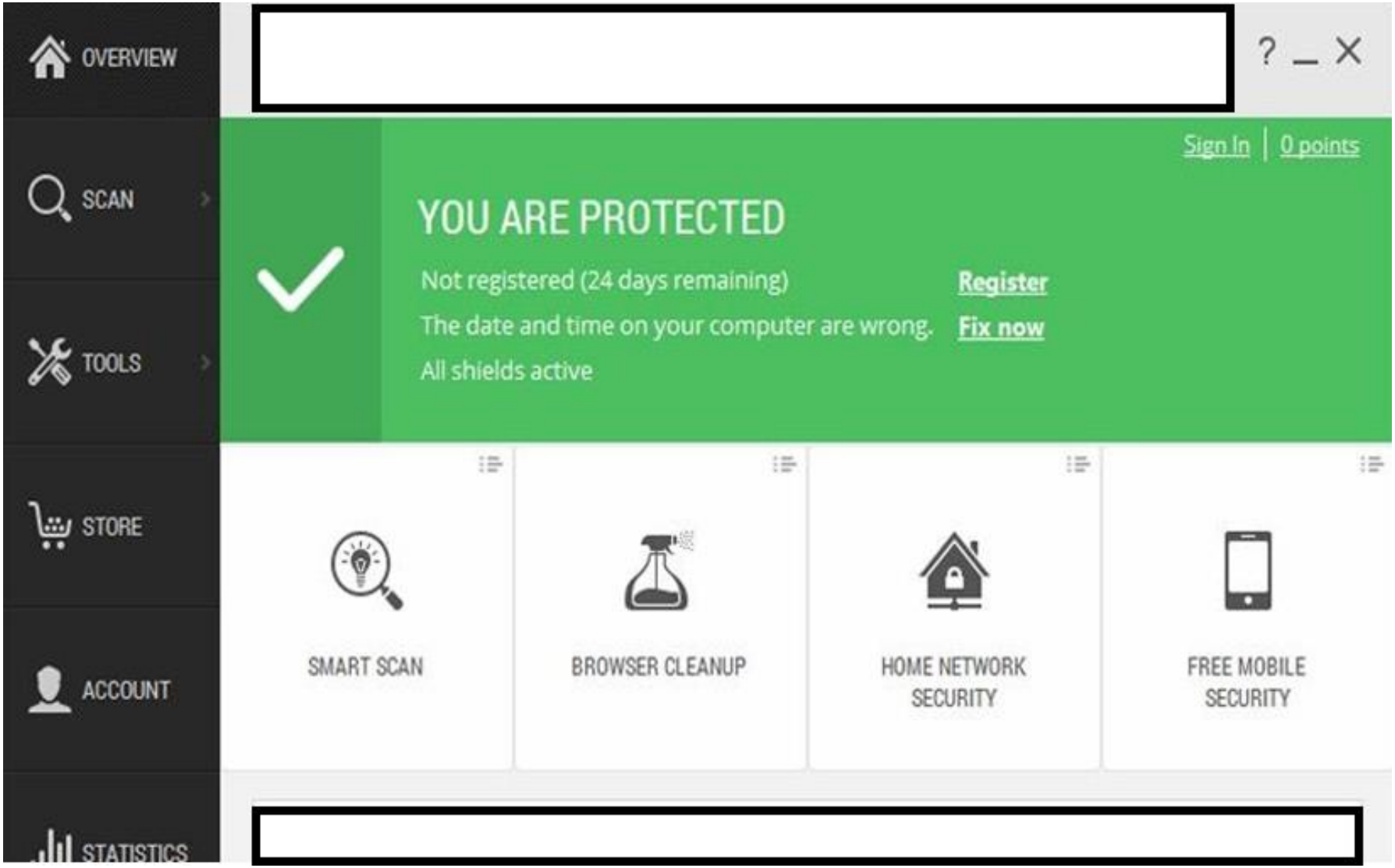
# You are seeing …

# Firewall Log: Connection Accepted…

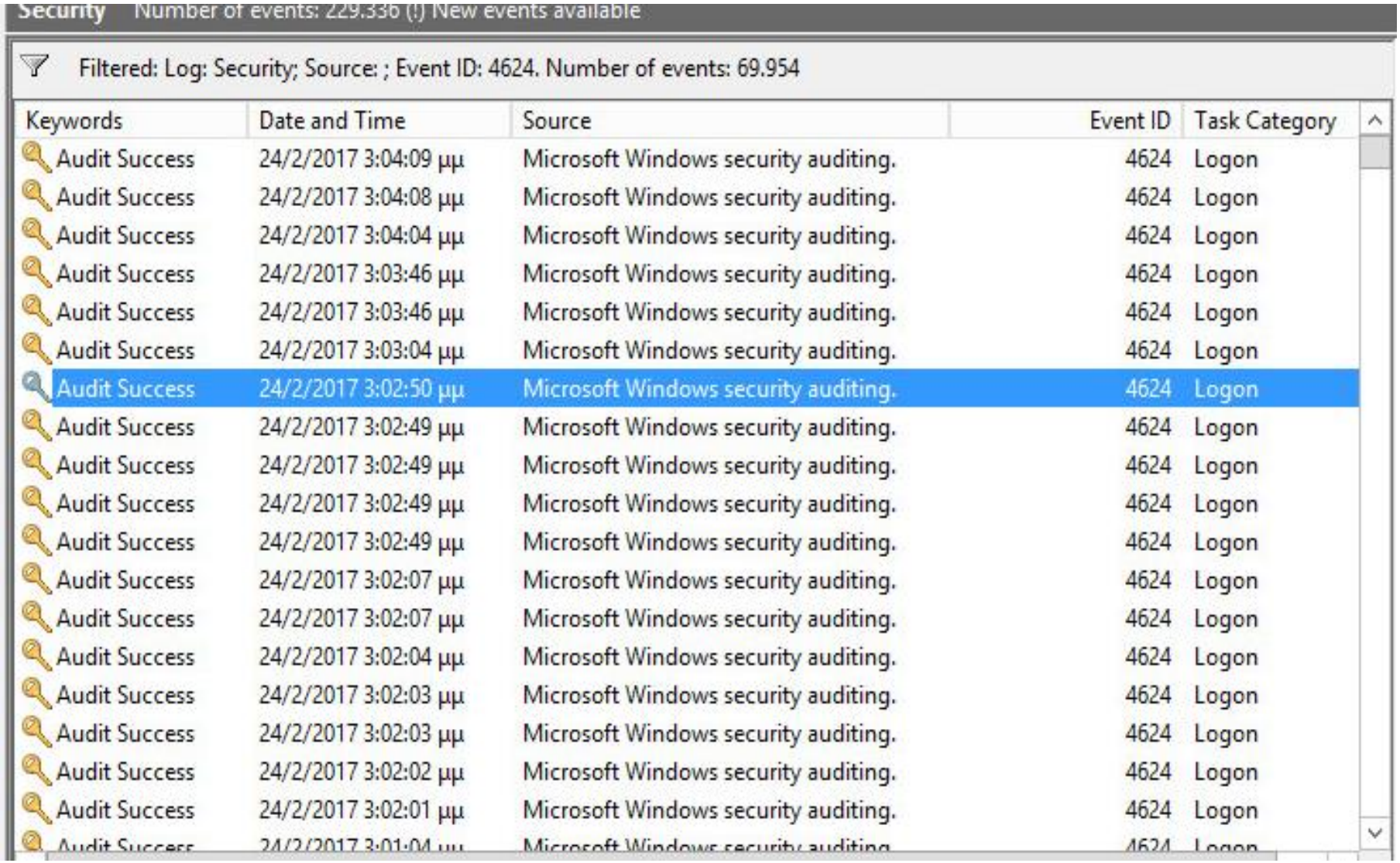


| No. | Date | Time | Origin | Service | Source | Source User Name | Destination | Rule |
|---|---|---|---|---|---|---|---|---|
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | UDP ntp-udp | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP IMAP-SSL | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP IMAP-SSL | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 17 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 17 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 17 |
| 2499… | 24Feb2017 | 14:23:19 | | UDP ntp-udp | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP ssh | | | | 17 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP http | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | TCP https | | | | 18 |
| 2499… | 24Feb2017 | 14:23:19 | | ICMP | | | | 17 |

# Antivirus: You Are Protected…



# Domain Controller: Logon Success…

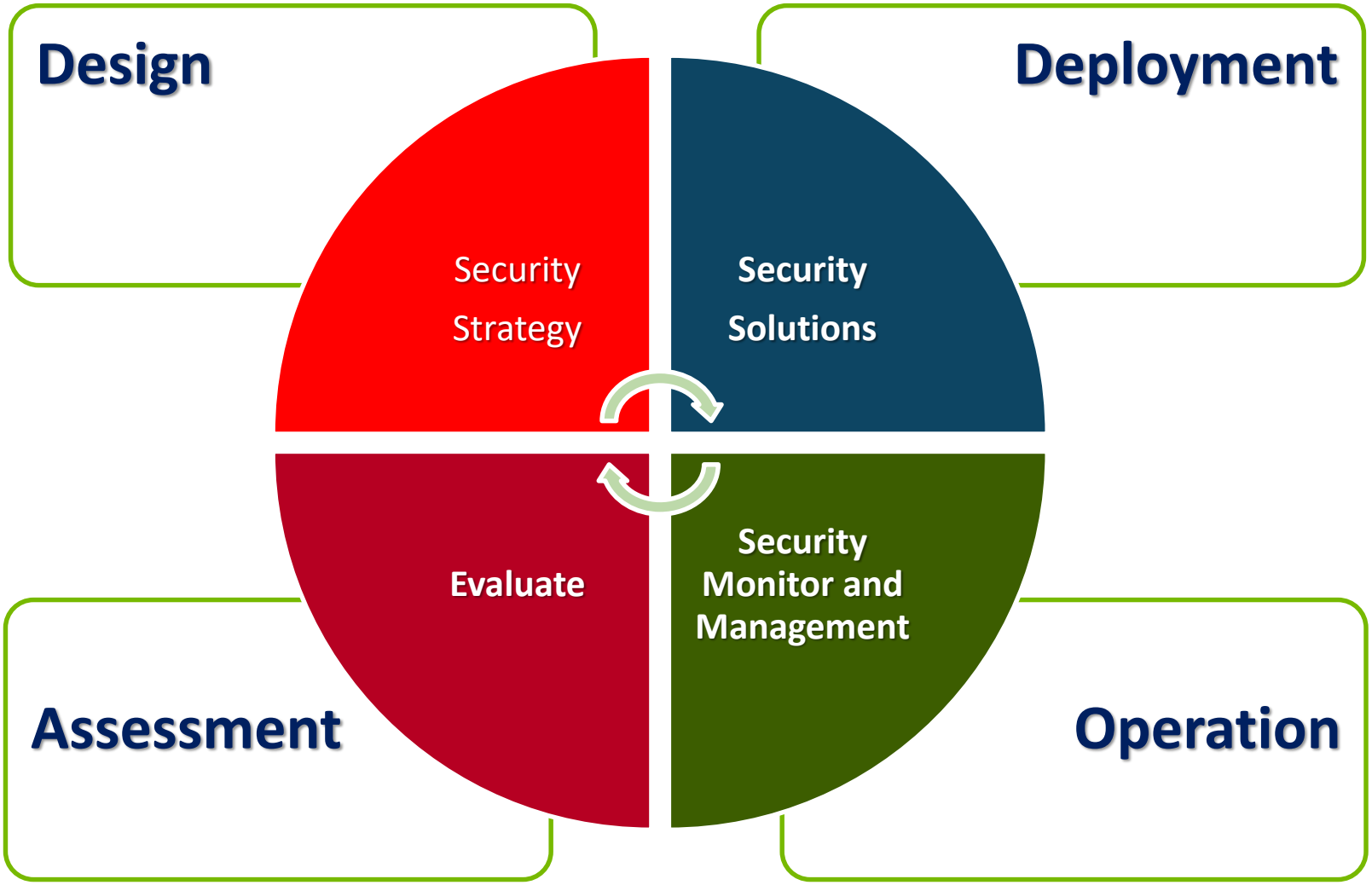


# Data: Protected

# You actual facing …

# The impact

# Our Approach:
## Follow security lifecycle



# Design a Security Strategy

## Risk Analysis

## Security Policy

1. Understand the cyber security risk

2. Integrate across personnel, technical security, information assurance and physical security

3. Establish protective monitoring to prevent and deter the 'insider' threat

4. Accept that some attacks will breach your defences – and plan on this basis

## Privacy Impact Assessment

# Deployment

## Netbull 3D Security Architecture (nSA 3D)


nSA: netbull 3D* Security Architecture

# On going Operation

- 24x7 Real Time Monitor
- Incident Management
- Advance Threat Management
- Security as a Service

# 24x7 Real Time Monitor

- Security events are analysed 24x7x365 by our Security Analysts and provides alerts when a security incident is detected.

- In the case of a real incident, our Analysts provides all necessary information as well as recommendations for the incident on its handling.

# Incident Management

## Our Security Experts:

- provide Emergency Incident Response Services within minutes of a validated security breach.

- work to contain the breach, mitigate the threat and protect your assets.


**As a result, we minimize the duration and impact to your organization from an active cyber security breach.**

# Advance Threat Management

- Netbull' Advanced Threat Management service provides an elite layer of defense against emerging zero-day threats.

- Using our platform, once a file lands on the endpoint, we continues to watch, analyse, and record file activity.

**When malicious behaviour is detected, it shows the recorded history of the threat's behaviour over time.**

# Security as a Service

- Device Management
- Upgrades
- Policy Management

# Our Technology:
## Netbull Threat Management Platform

- Threat Intelligence
- Early Warning
- IBM Q Radar
- Vulnerability Management
- User Behavior Analysis
- Malware Trap Hosts

# Evaluation (Regular Assessments)

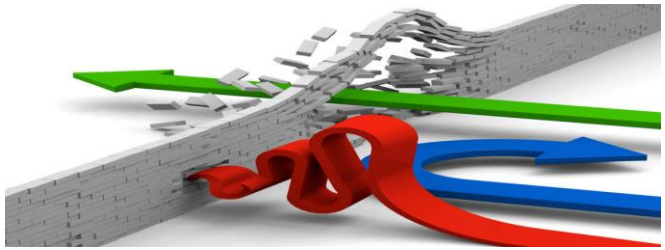
01 Planning phase, where the testing goals are set.

02 Discovery phase, covers information gathering, scanning and vulnerability analysis.

03 Attack phase, is the execution of the attacks, the heart of any penetration test.

04 Reporting phase, occurs simultaneously with the other three phases.

NIST



OWASP
The Open Web Application Security Project

# … for further information


Visit our website: www.netbull.gr