GJØVIK UNIVERSITY COLLEGE

Security planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 17.03.14

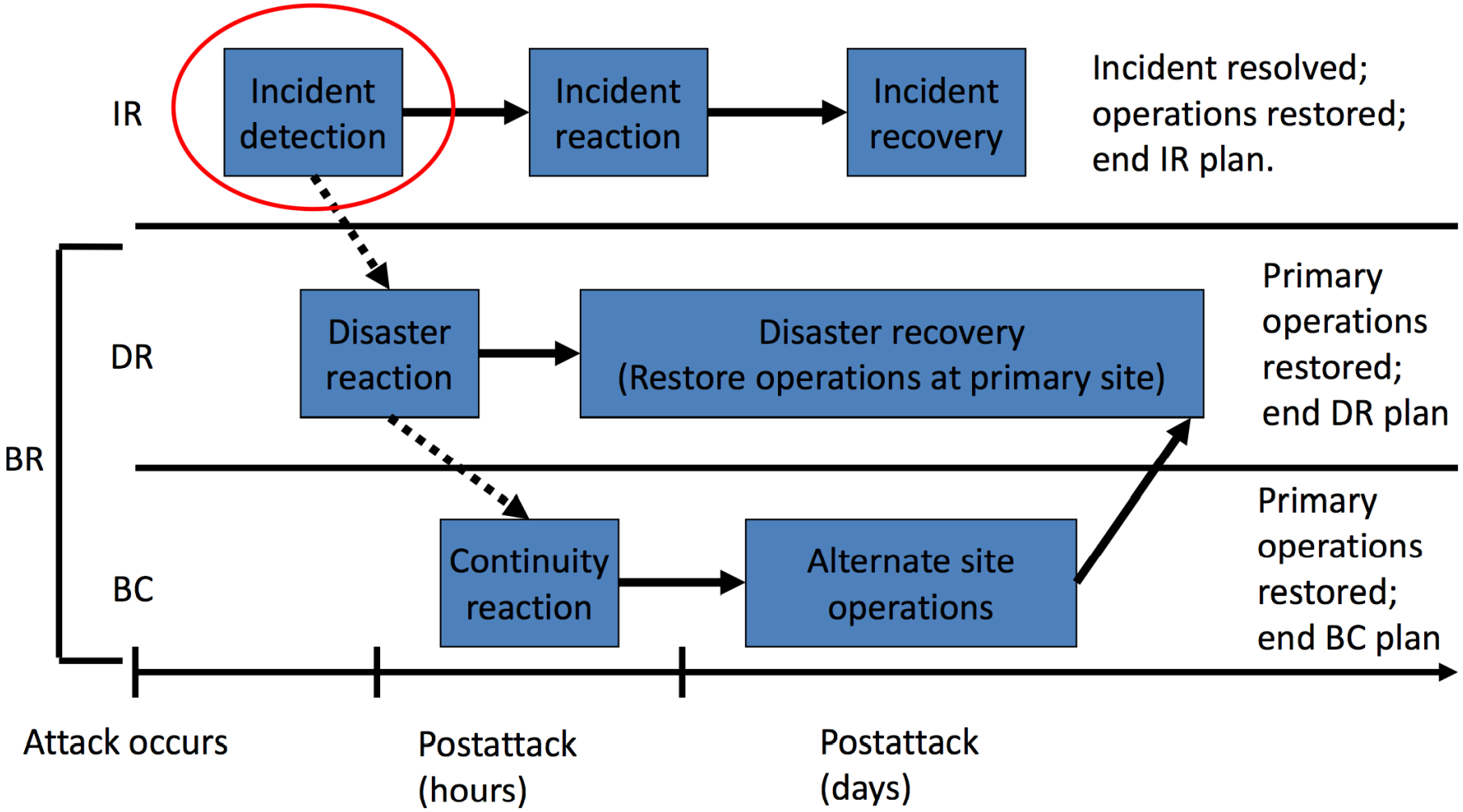
AGENDA

Incident Response: Detection and Notification

- *Incident Classification*
- *Intrusion Detection and Prevention Systems*
- *Incident Decision Making*

Services and Tools for Intrusion Detection

- *Proactive versus Reactive Detection*
- *Tools and Mechanisms*
- *Data feeds*
- *Hands on demo using Security Onion*



Whitman and Mattord 2007, p. 27

INCIDENT DEFINITION

Event:

Any observable occurrence in a system or network.

Adverse event:

An event with negative consequences.

Incident:

Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Source: NIST SP 800-61 rev. 2

INCIDENT CLASSIFICATION

Denial of service
- An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources

Malicious code
- A virus, worm, Trojan horse, or other code-based ,alicious entity that successfully infects a host

Unauthorized access
- When a person, without permission, gains logical or physical access to a network, system, application, data or other IT resource

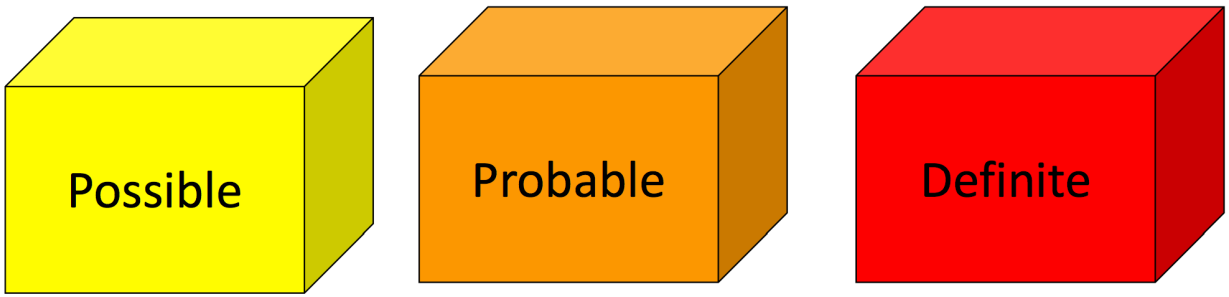
Inappropriate usage
- When a person violates acceptable use of any network or computer policies

Multiple component
- A single incident that encompasses two or more incidents

Source: NIST

INCIDENT INDICATORS

- Incident candidate = Suspected incident
- Three classes of incident indicators:



Donald L. Pipkin, Information Security: Protecting the Global Enterprise (Upper Saddle River, NJ: Prentice Hall PTR 2000), p. 256. Also Whitman and Mattord 2007, p. 131-135

POSSIBLE INDICATORS OF AN INCIDENT

1.Presence of unfamiliar files

2.Presence or execution of unknown programs or processes

3.Unusual consumption of computing resources

4.Unusual system crashes

PROBABLE INDICATORS OF AN INCIDENT

1. Activities at unexpected times
2. Presence of unexpected new accounts
3. Reported attacks
4. Notification from IDS

DEFINITE INDICATORS OF AN INCIDENT

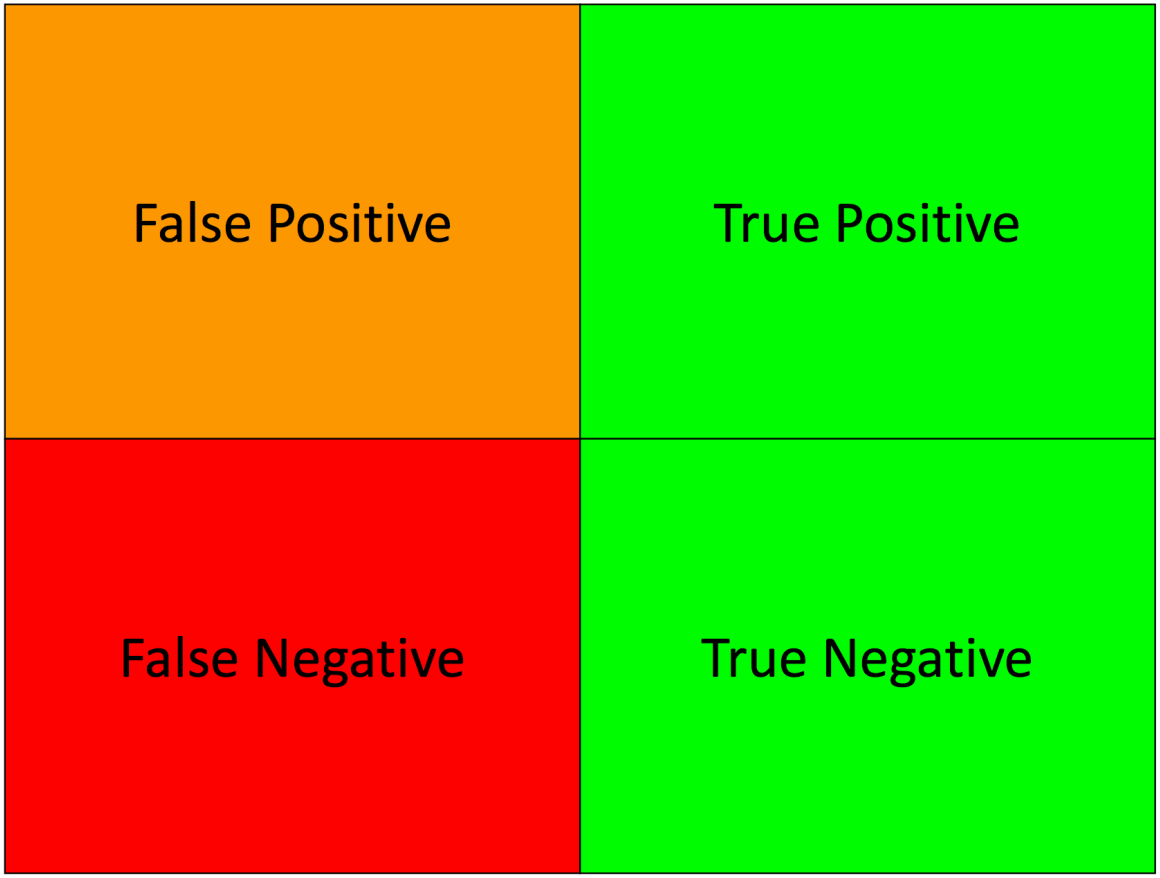
1. Use of dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notification by partner or peer
5. Notification by hacker

ALTERNATIVE INDICATORS

- Loss of availability
- Loss of integrity
- Loss of confidentiality
- Violation of policy
- Violation of law

Source: Whitman, Mattord and Green 2014, p. 172

IDENTIFYING REAL INCIDENTS



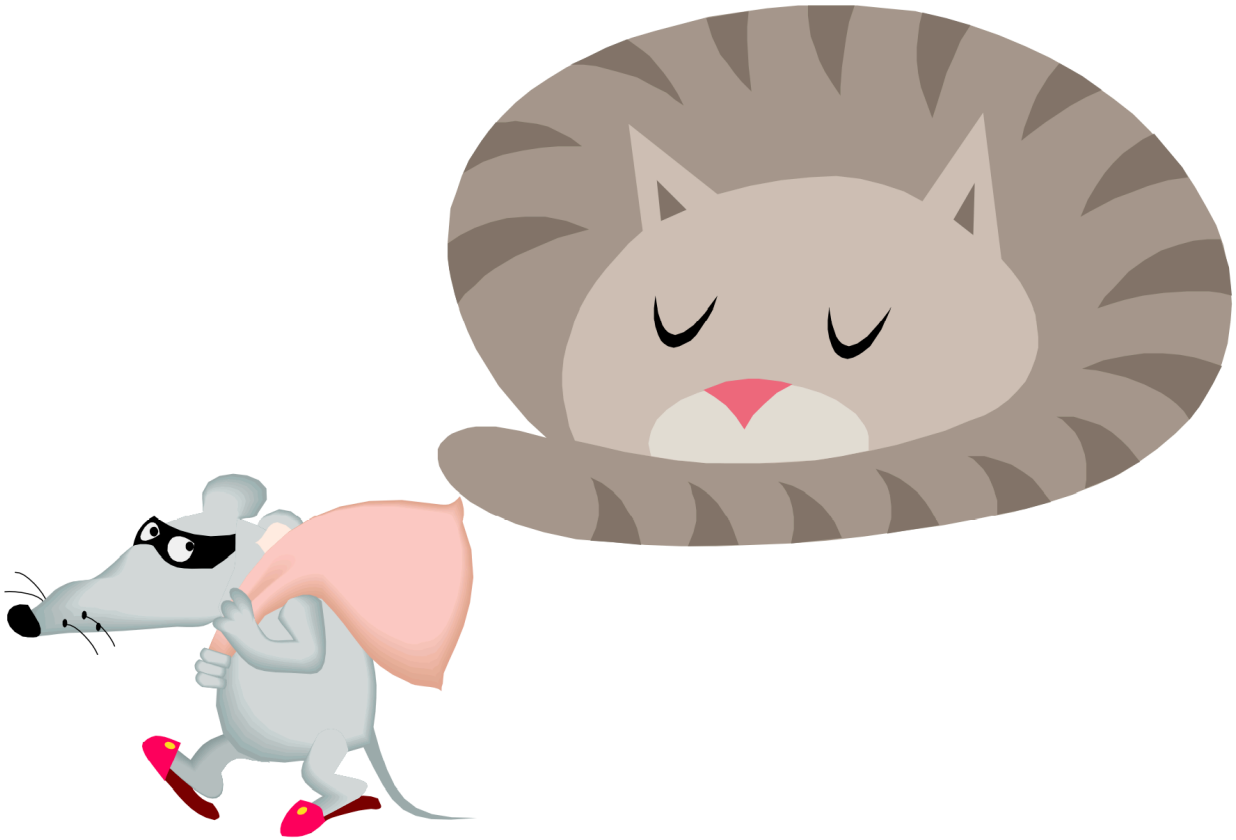
SOURCES OF FALSE POSITIVES

Placement
- IDS outside trusted sub-network

Policy
- Allowed activities create network signatures that are classified as malicious by IDS

Lack of awareness
- Users are unaware that certain actions are prohibited

FALSE NEGATIVES



INTRUSION DETECTION AND PREVENTION SYSTEMS

IDS: Intrusion Detection System

- Detects an intrusion or intrusion attempt and activates an alarm
- The system administrator may be alerted, e.g. by e-mail, or an external security service provider may handle the alerts

IPS: Intrusion Prevention System

- Detects intrusion attempts and prevents that intrusion from becoming a successful attack by active response

IDPS: Combined term used to describe current anti-intrusion technologies

Source: Whitman, Mattord and Green 2014, p. 182

IPS RESPONSE TECHNIQUES

- **The IPS stops the attack itself**
  - Terminate network connection or user session that is being used for the attack
  - Block access to the target from the offending user account, IP address, or other attacker attribute
  - Block all access to the targeted host, service, application, or other resource
- **The IPS changes the security environment**
  - Change the configuration or other security controls
  - Network configuration, firewall settings or patching of vulnerabilities
- **The IPS changes the attack's content**
  - Remove or replace malicious file attachments to e-mails
  - The IPS acts as a proxy and normalizes incoming packets

Source: NIST SP 800-94

IDPS TERMINOLOGY

- **Alert or alarm**: Attack indication
- **Alarm clustering**: Consolidation of almost identical alarms into a single higher-level alarm
- **Alarm compaction**: Alarm clustering based on frequency, similarity in attack signatures, similarity in attack target or other similarities
- **Alarm filtering**: Automatically filter alarms to sort false positives from actual attacks
- **Confidence value**: A value associated with an IDPS' ability to detect and identify an attack correctly
- **Evasion:** The process by which an attacker changes the format of network packets and/or timing to avoid being detected by the IDPS

IDPS TERMINOLOGY

- **False attack stimulus**: Event triggers alarm and triggers false positive
- **False negative**: Failure of IDPS to react to attack
- **False positive**: Attack indicated when no attack is in progress
- **Filtering**: Reducing IDPS events in order to receive a better confidence in the alerts received
- **Noise**: accurate but not significant alerts. Probes, scans, employees using scanning tools
- **Site Policy**: Rules and configuration guidelines governing implementation and operation of IDPS
- **Site policy awareness**: Ability of the IDS to modify its site policies in reaction to environmental activity
- **True attack stimulus**: An event that triggers an alarm
- **Tuning**: Adjusting an IDPS to maximize its efficiency in detecting true positives while minimizing both false positives and false negatives

IDPS NETWORK PLACEMENT

Network-based IDPS (NIDPS)

- Resides on a network segment and monitors traffic on that segment

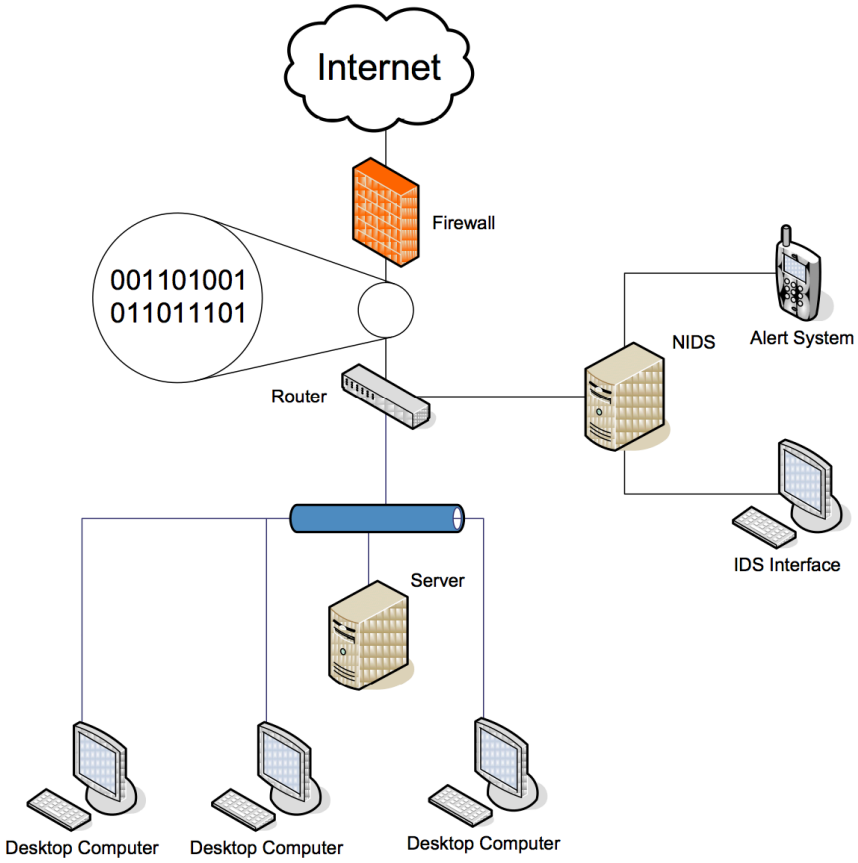
Host-based IDPS (HIDPS)

- Resides on a particular computer or server, known as the host, and monitors activity only on that system

Application-based IDPS (AppIDPS)

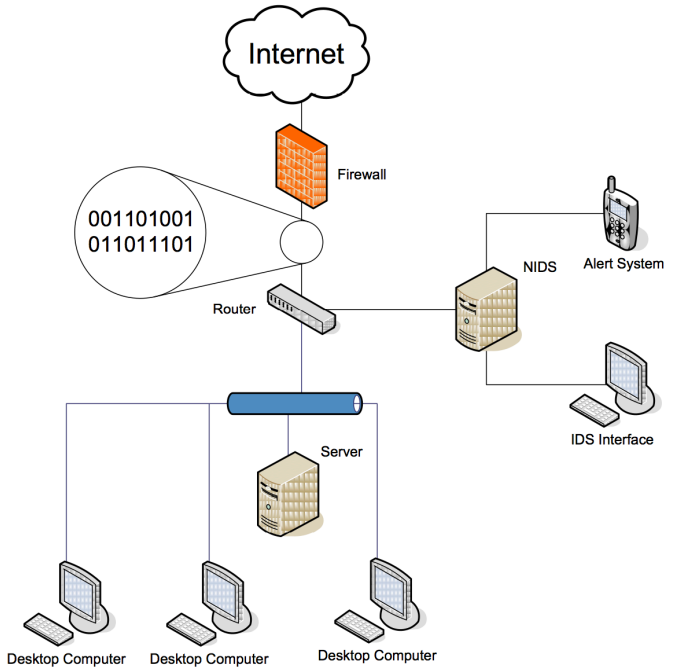
- Resides on a host and examines an application for abnormal events

NETWORK-BASED IDPS (NIDPS)



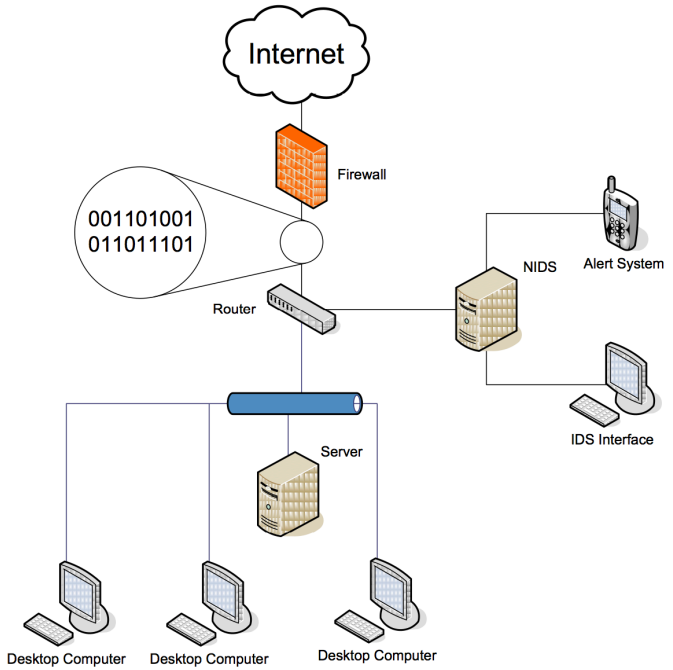
NIDPS ADVANTAGES

- Few devices can monitor large network
- Usually passive, can be deployed without disturbing normal network operations
- Not usually susceptible to direct attack, may not be detectable by attackers

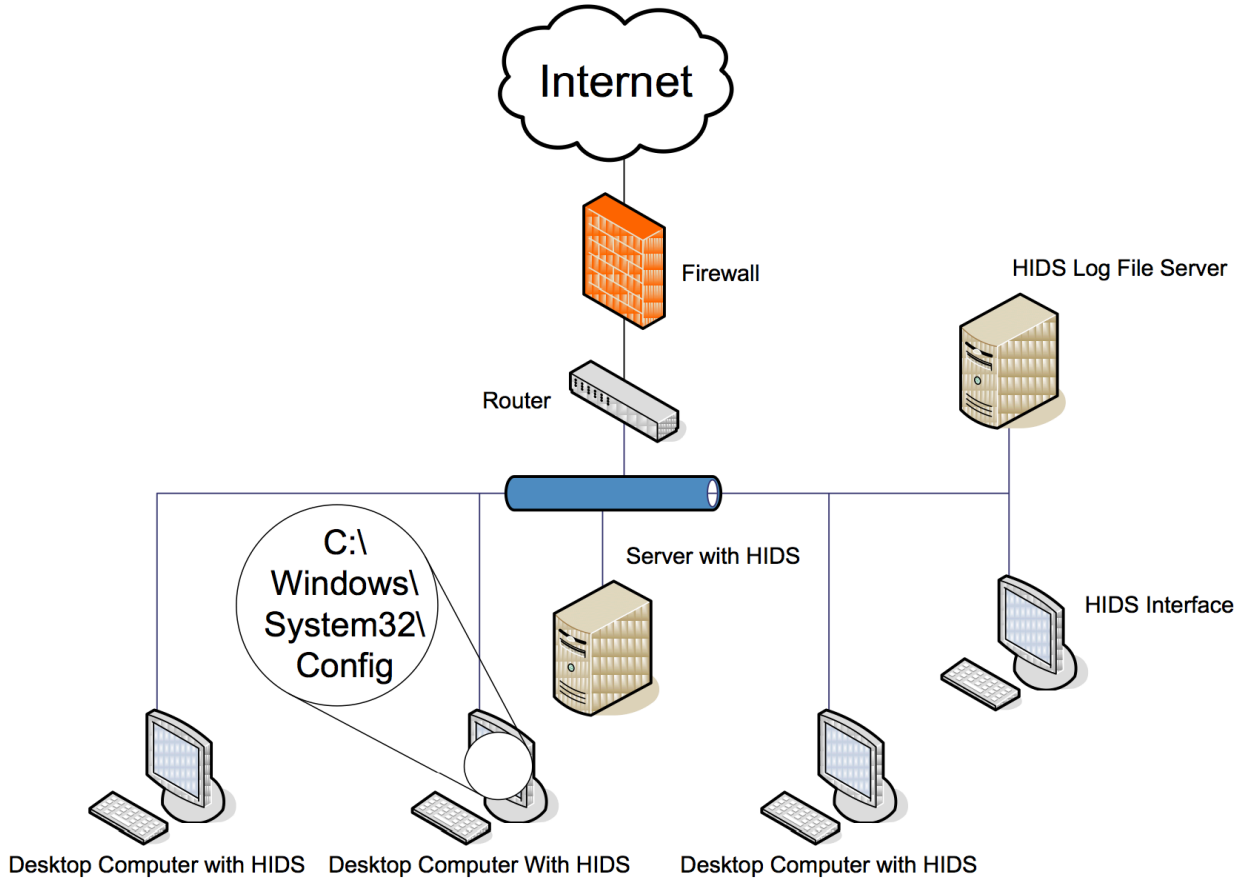


NIDPS DISADVANTAGES

- Can become overwhelmed by network volume and fail to recognize attacks.
- Requires access to all traffic to be monitored. Requires switches to have monitoring ports.
- Can not analyse encrypted data packets, some of the network traffic is invisible.
- Can not reliably determine whether an attack was successful. Administrator must manually evaluate.
- May have trouble with fragmented or malformed packets.

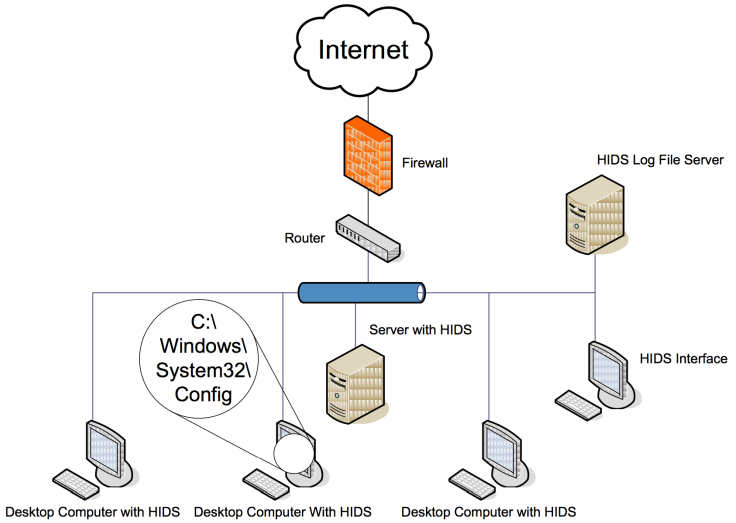


HOST-BASED IDPS (HIDPS)



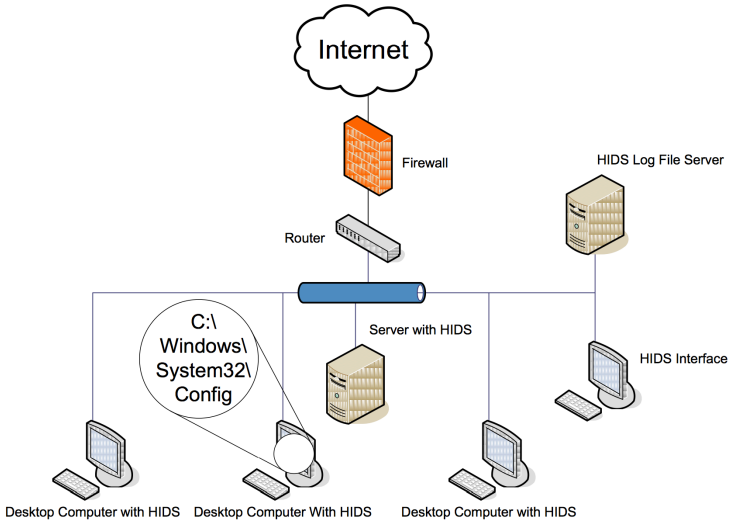
HIDPS ADVANTAGES

- Can detect local events on host systems and attacks that elude NIDS.
- Encrypted traffic is decrypted on the host system, allowing HIDS to inspect it.
- Not affected by switched network protocols.
- Can detect inconsistencies in how applications and programs were used by examining logged records.

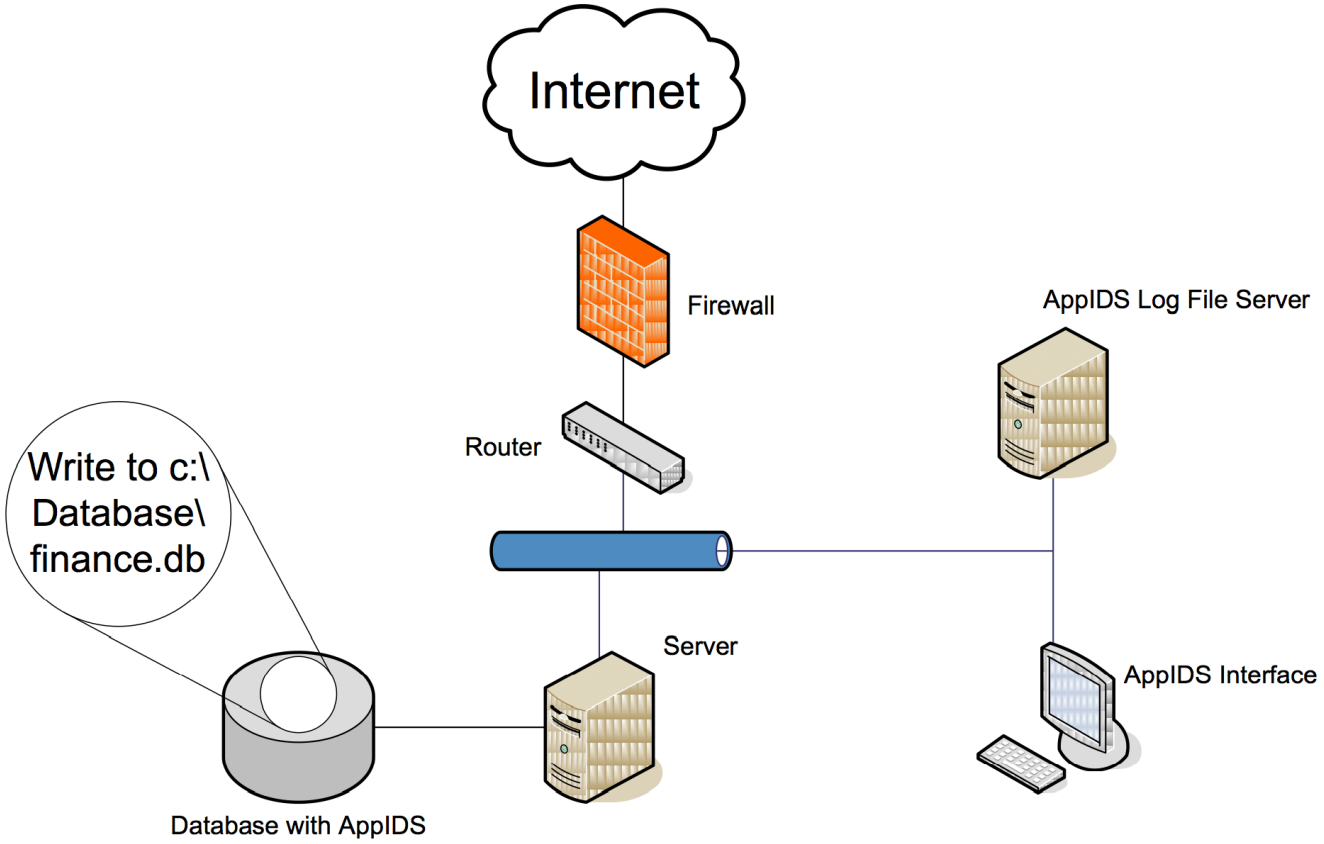


HIDPS DISADVANTAGES

- Requires more effort as HIDPS are configured and managed on each host.
- Vulnerable to direct attacks and attacks against host system.
- Not optimized to detect multi-host scanning, nor able to detect scanning of non-host network devices, unless complex correlation analysis is provided.
- Can use large amounts of disk space to retain host OS audit logs.
- Can inflict performance overhead on its host systems to below acceptable levels.
- Susceptible to some denial-of-service attacks.

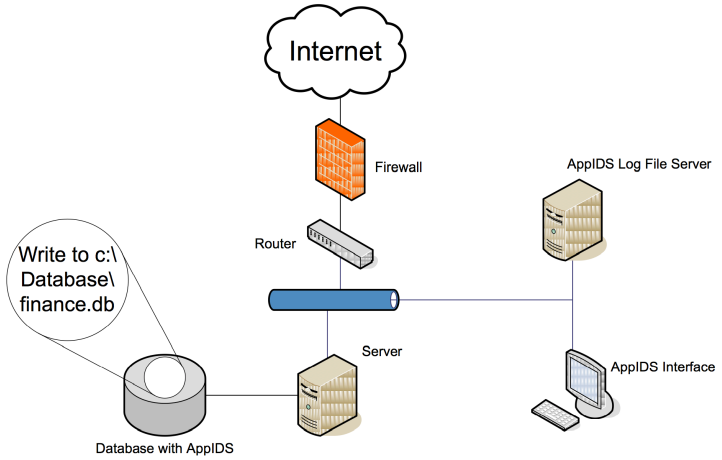


APPLICATION-BASED IDPS (APPIDPS)



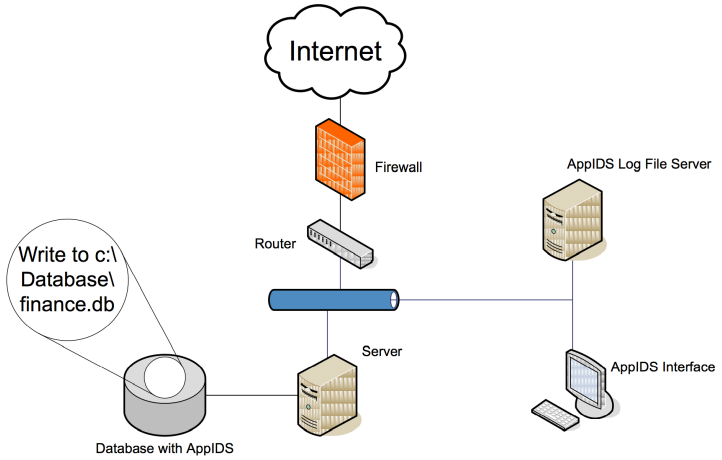
APPIDPS ADVANTAGES

- Is aware of specific users and can observe the interaction between application and user.
- Can operate when incoming data is encrypted, as it can operate at the point in the process where data has been decrypted and not yet been encrypted for storage.



APPIDPS DISADVANTAGES

- Applications are often less protected than network and host OS components. May make AppIDPS more vulnerable than other IDPS.
- AppIDPS is less capable of detecting software tampering and may be taken in by Trojan horse code or other form of spoofing.



IDPS DETECTION APPROACHES

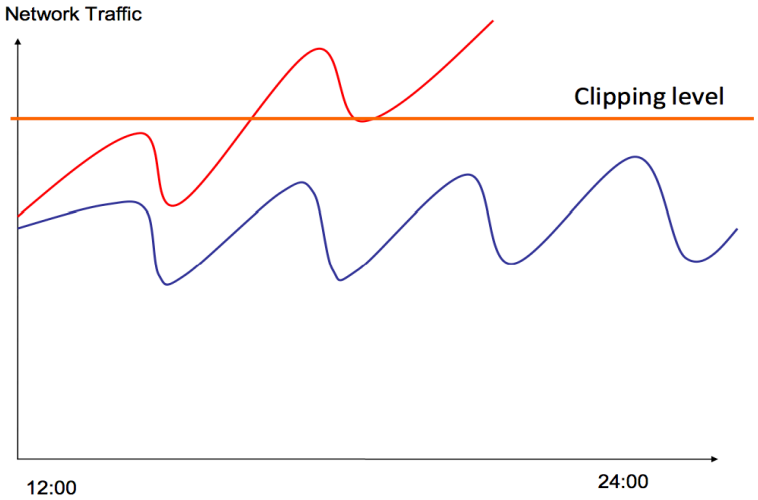
- Signature-based IDPS
- Anomaly-based IDPS
- Log File Monitors
- Automated Response (Trap and Trace)
- Honeypots and Honeynets

SIGNATURE-BASED IDPS

- Also known as knowledge-based IDS
- Examines data traffic in search of patterns that match known signatures
- Footprinting and fingerprinting includes the use of ICMP, DNS querying and e-mail routing analysis
- Traditional antivirus software can be considered a signature based IDPS
- The IDPS's database of signatures must be continually updated as new attack strategies are identified

ANOMALY-BASED IDPS

- Also known as behaviour-based IDS.
- Collects statistical summaries by observing network traffic known to be normal.
- Then compares normal standard to actual traffic. Gives warning if clipping level is exceeded (actual traffic differs sufficiently from baseline).
- Can detect new types of attacks.
- Require much more overhead and processing capacity than signature-based IDPS.
- May generate many false positives.



LOG FILE MONITORS (LFM)

- Reviews log files generated by servers, network devices and other IDPSs.
- Looks for patterns that indicate an attack or intrusion is in progress or has already succeeded.
- E.g., keycard system logged user as exiting building 3 hours ago, but same user just logged in locally to database server.
- Requires allocation of considerable resources, as it involves the collection, movement, storage and analysis of very large quantities of data.

AUTOMATED RESPONSE (TRAP AND TRACE)

- Systems that autonomously react to incidents, based on preconfigured options
- Uses a combination of resources to detect an intrusion and then trace it back to its source
- "Hacking back" poses huge ethical problems:
  - *Attackers often use innocent dupes as stepping stones for attacks*
  - *IP spoofing, compromised systems as stepping stones, and a myriad of other techniques are available to the hacker*
  - *In tracing the intrusion you may be committing an intrusion yourself*

HONEYPOTS AND HONEYNETS

Honeypots

- A closely monitored network decoy.
- Can distract adversaries
- Can provide early warning of new attacks
- Allows in-depth examination of adversaries during and after exploitation

Honeytoken

- A single dummy file placed in a system. This file should not be read or written to. If this occurs it is most likely due to unauthorized or malicious activity.

Honeynets

- Same as honeypot, except it is a network rather than a single machine.
- High-interaction, provides real systems, applications and services for attackers to interact with

LEGAL ISSUES WITH HONEYPOTS AND HONEYNETS

Entrapment: luring a person into committing a crime to get a conviction.

Enticement: Attracting attention to the system by placing tantalizing bits of information in key locations.

- Entrapment is forbidden in many countries.
- Other legal issues relate to interception of electronically transmitted communication.
- Laws vary from country to country. You should seek legal advice before employing honeypots and honeynets.

INCIDENT DECISION MAKING

1.Collect incident candidates using well- documented procedures

2.Investigate the candidates using systems and methods at your disposal

3.If an incident is determined, initiate incident response procedures

RECOMMENDED PRACTICES FOR IDPS IMPLEMENTATION

Planning

- Develop/verify policies, procedures, and processes to detect indications of intrusion
- Prepare a business impact analysis to define systems and relative importance
- Ensure system and network logs are enabled, collected and consolidated for analysis

IDPS Integrity

- Validate the IDPS is reliable, accurate and uncompromised

Network and System Baseline

- Monitor the following for unexpected change and unusual behaviour:
  - Network activities
  - System activities and configurations
  - Directory and file systems

RECOMMENDED PRACTICES FOR IDPS IMPLEMENTATION

Physical controls

- Validate/update the hardware inventory
- Verify physical integrity of work and storage spaces
- Investigate unauthorized hardware attached to your organisation's network

Implementation

- Ongoing detection activities to review IDPS, help desk, and other reports of suspicious activities
- Act on notifications to triage and then escalate and respond to warranted events including unauthorized, unexpected, or suspicious activity

MANAGE LOGGING AND OTHER DATA COLLECTION ACTIVITIES

- Be prepared to handle huge amounts of data.
- Rotate logs on schedule, some systems overwrite old logs.
- Archive logs or risk losing ability to investigate. How long depends on purpose and the law.
- Encrypt logs
- Dispose of logs securely once they have outlived their usefulness.

MONITOR THE NETWORK FOR UNEXPECTED BEHAVIOUR

- Notify users that network monitoring is being done.
- Review and investigate notifications from network-specific alert mechanisms (e-mail, voice mail, etc.)
- Review and investigate network error reports.
- Review network performance statistics and investigate apparently anomalous behaviour.
- Identify unexpected, unusual or suspicious network traffic and its possible implications
- If you are reviewing network traffic on a system other than the one being monitored, ensure that the connection between them is secure.

MONITOR SYSTEMS FOR UNEXPECTED BEHAVIOUR

- Notify users that monitoring of process and user activities is being done.
- Review and investigate notifications from system-specific alert mechanisms (e-mail, voice mail, etc.)
- Review and investigate system error reports.
- Review system performance statistics and investigate apparently anomalous behaviour.
- Continuously monitor process activity (to the extent that you can)

MONITOR SYSTEMS FOR UNEXPECTED BEHAVIOUR

- Identify unexpected, unusual or suspicious user behaviour and its possible implications.
- Identify other unexpected, unusual or suspicious behaviour and its possible implications.
- Periodically execute network mapping and scanning tools to understand what intruders who use such tools can learn about your network and systems.
- Periodically execute vulnerability scanning tools to check for the presence of known vulnerabilities.
- If you are reviewing system activities on a host other than the one being monitored, make sure the connection is secure.

MONITOR FILES AND DIRECTORIES FOR UNEXPECTED CHANGES

- HIDPS is the most effective way of doing this.
- Can (should) be augmented by having a reporting process in place to allow users to alert the monitoring team of suspicious file activity.

INVESTIGATE UNAUTHORIZED HARDWARE ATTACHED TO THE NETWORK

- Existing software can scan the network and identify type, location and configuration of network devices.
- Visual inspection should also be periodically performed.
- Unauthorized equipment may tap into the system and redirect or record traffic.

INVESTIGATE PHYSICAL RESOURCES FOR SIGNS OF UNAUTHORIZED ACCESS

- Physical access trumps electronic security.
- Intruders can remove hard drives, optical storage media, laptops, desktops, etc.
- Intruders may also install malware or unauthorized hardware

REVIEW REPORTS ABOUT SUSPICIOUS OR UNEXPECTED BEHAVIOUR

- The users are your front line foot soldiers for intrusion detection.
- They can detect suspicious or unauthorized behaviour that computers can not. E.g., social engineering.
- Good communication between CSIRT and users improve user awareness.

PROACTIVE VERSUS REACTIVE DETECTION

Proactive detection of incidents is the process of discovery of malicious activity in a CERT's constituency through internal monitoring tools or external services that publish information about detected incidents, before the affected constituents become aware of the problem.

Proactive detection of incidents can be viewed as a form of an **early warning service** from the constituents' point of view

Source: Proactive Detection of Network Security Incidents, ENISA Deliverable

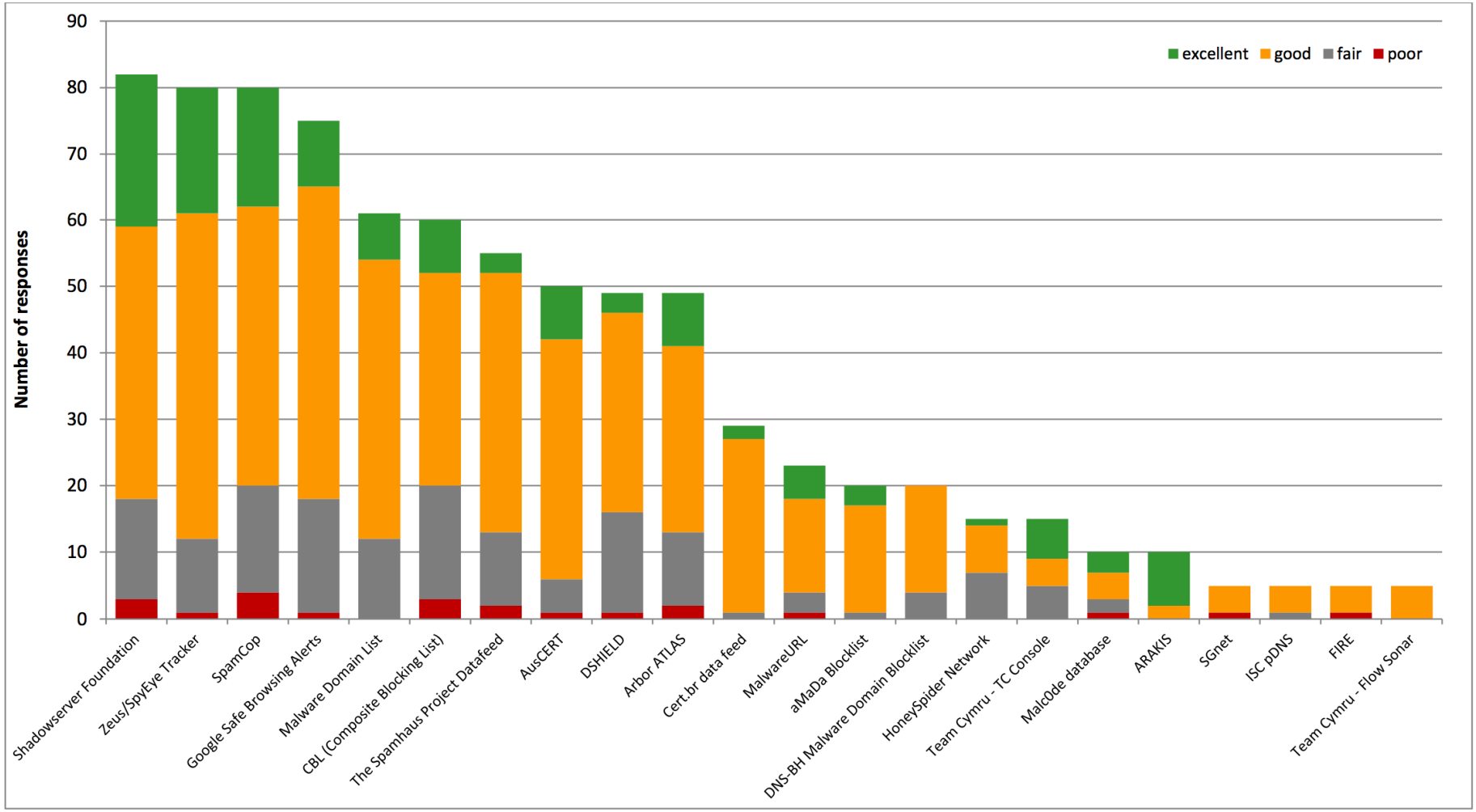
DIFFERENT APPROACHES FOR PROACTIVE DETECTION

Tools that can be **deployed by a CERT** to internally monitor events in its constituency.

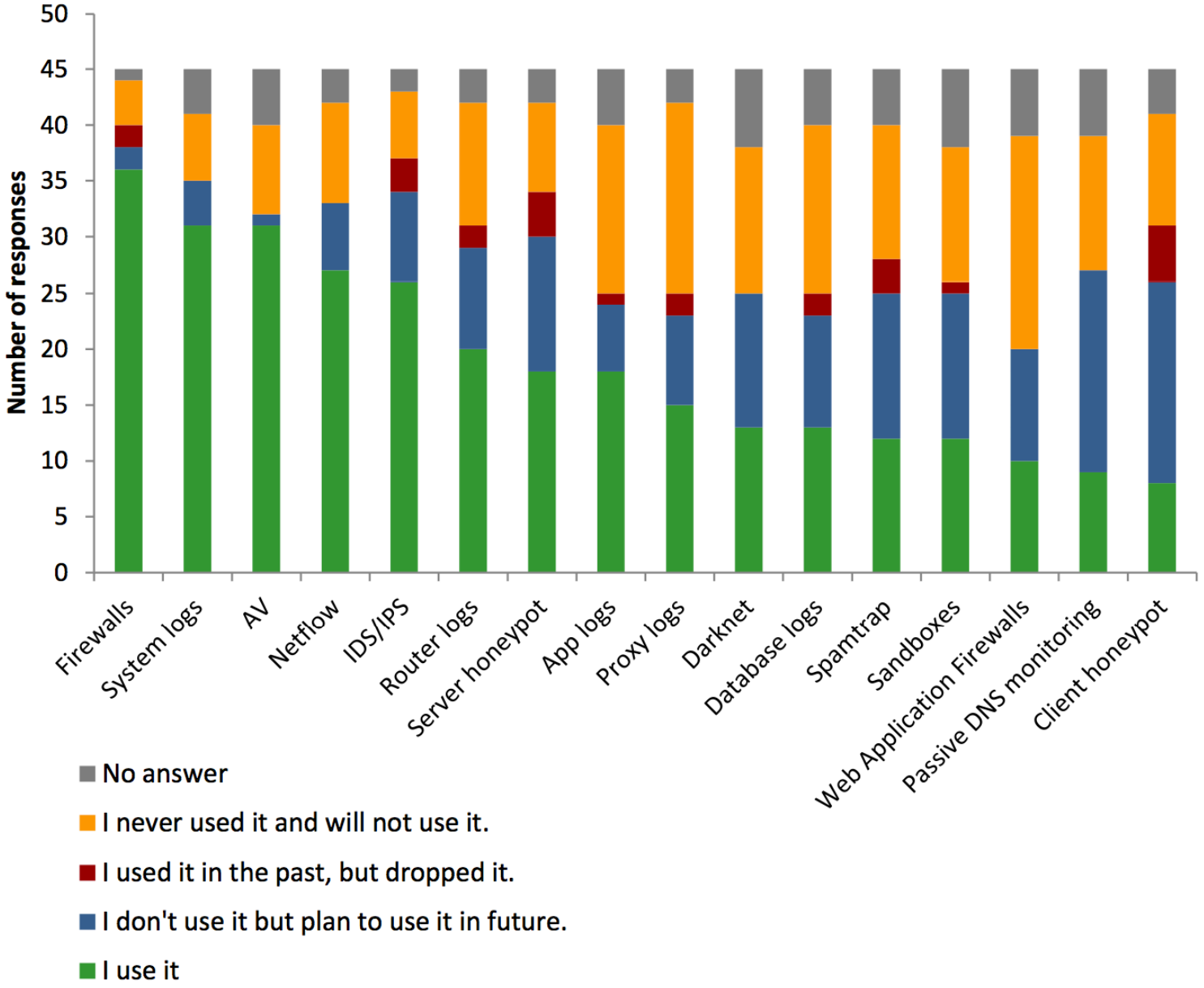
- IDPS
- Netflow
- Honeypots and Honeynets
- Antivirus solutions
- Log monitoring

Services that have been made available on the Internet which provide information about detected network security incidents to affected parties.

- Public, closed or commercial sources
- Data feeds are run by various security organisations, projects, vendors, universities, CERTs or non-profit initiatives, or even enthusiastic individuals
- Data feeds may include IP addresses, URLs, domains or malware associated with a particular malicious activity, such as a bot, C&C server, malicious URL or scanning
- Sometimes more sensitive data are offered – such as stolen user credentials or credit card data



Source: Proactive Detection of Network Security Incidents, ENISA Deliverable



Source: Proactive Detection of Network Security Incidents, ENISA Deliverable

TOP 'MUST HAVE' TOOLS (AND MECHANISMS)

Standard tools/mechanisms

- Routers, firewalls, antivirus systems, IDPS, netflow and various kinds of logs

Advanced tools/mechanisms

- Darknets, server honeypots, spamtraps and networks of sensors

Upcoming tools/mechanisms

- Client honeypots, sandboxes, passive DNS monitoring and analysis techniques

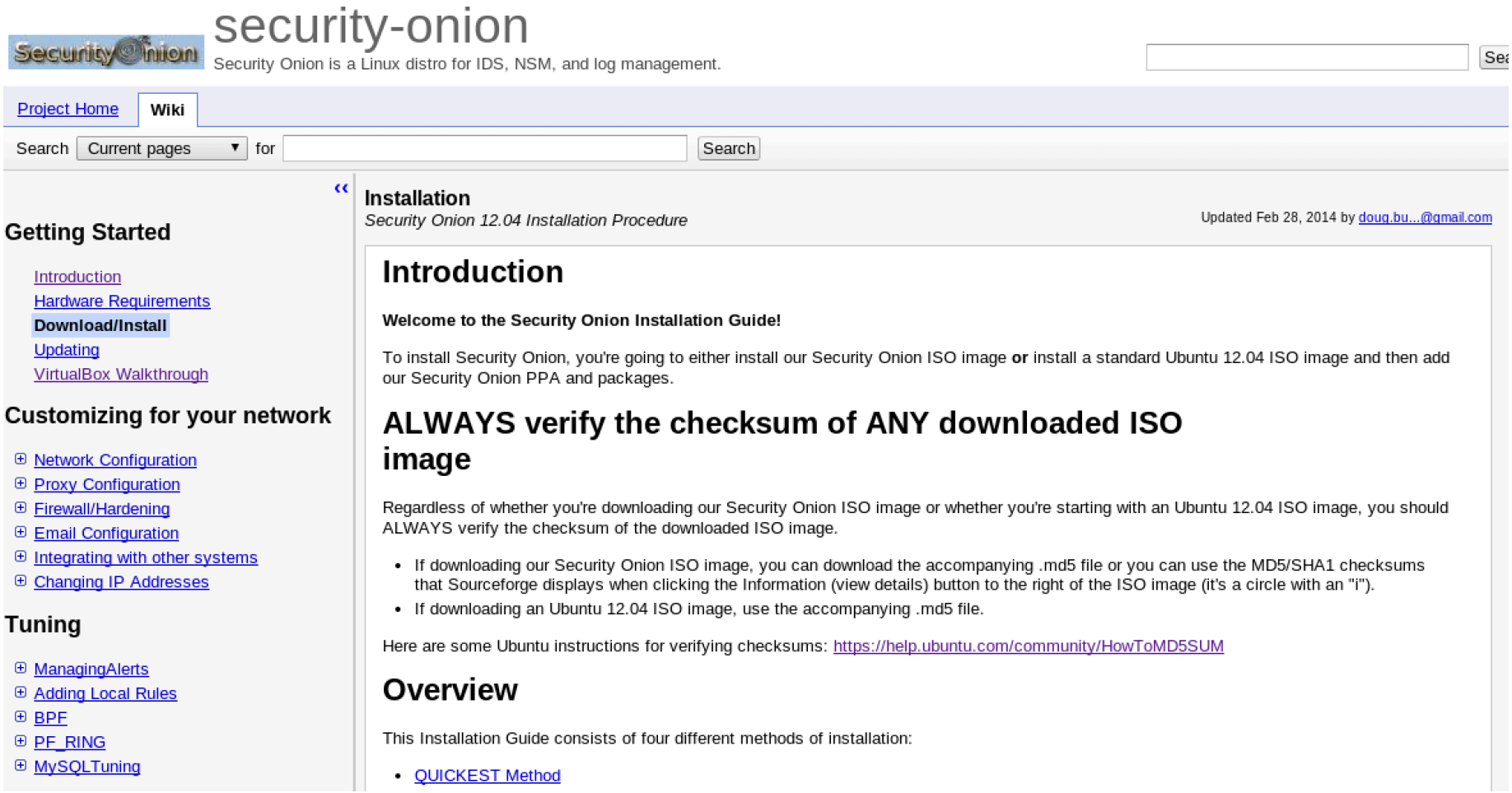
SOME SHORTCOMINGS IN PROACTIVE DETECTION

- Assessment of **false negative rates** for external services that supply security information is difficult
- Providers of information usually do not reveal from where and under what conditions the data were gathered.
  - Therefore the **context** in which an incident is detected by a data supplier is often unclear
  - This influences the perceived reliability of data.
- **Timeliness of delivery** to the receiving entity contributes to the perceived false positive rate of a data source.
- **Data aging** is another element of quality.
- **Lack of common formats**
- **Lack of correlation** of external services that provide incident data
- **Lack of automation** tools for data feed processing

SOME SHORTCOMINGS IN PROACTIVE DETECTION

- **Targeted attacks underreported**
  - No data feeds dedicated to information on more specific attacks against organisations
  - APT, digital espionage
- **Passive DNS monitoring underused**
- **Lack of services for data leak reporting**
- **Legal issues impede data sharing**
- **Lack of human resources**
- **Obstacles in reaching closed groups**

HANDS-ON DEMO



http://code.google.com/p/security-onion/wiki/Installation

for Search

« **IntroductionWalkthrough**

Installing SO in a Virtualbox VM and introduction to tools, configuration and workflow with Sguil.

Walkthrough

Security Onion is configured to run on version 12.04 of any Ubuntu-based Linux server or desktop distribution, such as Ubuntu, Lubuntu, Xubuntu, and Kubuntu. Your base operating system choice really depends on personal preference, your hardware and how you intend to interact with Security Onion. If you're experienced with the flavors of Ubuntu you probably have already made this decision. We're going to walkthrough setting up the Security Onion Live Xubuntu 12.04 distribution in a virtual machine (VM) and installing Security Onion using the Quick Setup option. Having Security Onion installed in a VM gives you an isolated environment which can act as a "client" for interacting with a remote Security Onion server. In an Ubuntu Server deployment, where access to the server is limited to SSH and command line, the client VM will let us setup remote servers and sensors graphically. It is also recommended for analysts to run Security Onion in a virtual machine for client access to ensure you have all the tools needed to manage and monitor a deployment in an isolated environment. You'll need a computer with at least 4GB of RAM (ideally 8GB) for best results. We'll use VirtualBox, a free desktop virtualization tool, but the process is very similar for VMware or others. You can download a copy of VirtualBox for Windows, Mac OS X or Linux at http://www.virtualbox.org. We'll also need to download the Security Onion 12.04 Live distribution from https://sourceforge.net/projects/security-onion/files/12.04/.

http://code.google.com/p/security-onion/wiki/IntroductionWalkthrough

SECURITY ONION FEATURES

- Signature-based NIDS:
  - Snort
  - Suricata
- Analysis-driven NIDS:
  - Bro
- Host-based IDS
  - OSSEC
- Analysis tools
  - Sguil – “The Analyst Console for Network Security Monitoring”
  - Sqert – Web application interface to the Sguil database
  - Snorby - Web application interface to Snort and Suricata alerts
  - ELSA - Enterprise Log Search and Archive

NEXT LECTURE

The topic of the next lecture on the 31th of Mars will be:

Incident Response: Reaction, Recovery and Maintenance

Recommended reading to prepare for the next lecture:

- Chapter 7 & 8 in Whitman, Mattord and Green

Please remember the **guest lecture by** Sven-Erik Egge from the Norwegian Government Security and Service Organisation IT Dept. (DSS):

22/7 How to handle a major crisis - From IT dept's perspective

- The talk will be held in K105 at 12:15-13:00 Friday 21th of Mars