

Security Monitoring

in an internet-enabled environment

Mirna Bognar

SAFE-NL, TU Eindhoven, 13 June 2003

**Deloitte
& Touche**

Overview

- Introduction:
information security, security management, security monitoring
- Security monitoring issues:
questions, incidents, sensitive objects, sources of information,
security monitoring environment
- Security monitoring activities:
logging, monitoring, reporting
- Roles in security monitoring
- Security guidelines

Background: Information security

- Information security defined in terms of
 - **confidentiality**: ensuring that information is accessible only to those authorised to have access
 - **integrity**: safeguarding the accuracy and completeness of information and processing methods
 - **availability**: ensuring that authorised users have access to information and associated assets when required

Security in computer environments

- Security in old-fashioned computer networks:
 - protection from internal users
 - account management, physical access control crucial
 - (security) monitoring performed by system administrators
- Security in internet-enabled networks:
 - protection from internal and external users
 - increased complexity of systems (networks, software), more vulnerabilities
 - exposure to attacks from Internet
 - security monitoring performed by security administrators
- Security management, i.e., safeguarding information security involves different aspects:
organisational, technical, procedural, legal...

Security monitoring

- controlling the security status of a computer environment w.r.t.
 - attacks from Internet
 - attacks/misuse from inside the environment (users, administrators, developers...)
 - reporting on security status
- providing a pre-context to incident response & recovery:
 - input for incident investigation
 - audit trail of the incident

Why security monitoring?

- safeguarding information is an integral part of services
- information security in terms of contracts with clients (including Service Level Agreements)
- company image:
 - positive – competitive advantage
 - negative – in case of major security incidents

Security monitoring issues

- the questions to be answered
- definition of incidents and respective priorities
- identification of sensitive objects (assets labeling)
- a security monitoring environment
- translation of questions into daily activities
- fine-tuning of the security monitoring, intrusion detection, data analysis (incl. correlation of events)
- management and security of security monitoring environment

Starting point: questions (1)

- **Accounts:**
 - creations of new accounts
 - number of new accounts as expected?
 - user rights?
 - any new administrators?
 - authorised?
- **Access:**
 - log-ons: users, administrators
 - account lock-outs
 - access to sensitive objects
 - physical access to environment

Starting point: questions (2)

- **Activities:**
 - software installations
 - patches/hotfixes installation
 - reboots
 - backup
 - configuration changes
- **Network traffic:**
 - normal quantity
 - internal network: unexpected protocols, IP addresses
 - attacks from the Internet, office network, system admin. segment

Starting point: questions (3)

- Security monitoring tools
 - logging services and tools operational?
 - configuration changes
- General
 - new-found vulnerabilities
 - abnormal behaviour
- Regular security scans
 - status of the network wrt security (patches, configuration changes etc)
 - trends in attacks, network traffic etc
 - review of operational procedures
 - risk assessments

Incidents

- Depending on environment, terms of contracts with clients...
- E.g.

Incident	Priority	Examples
Client data compromised	1 (high)	OS control over any component
No client data compromised, but the company's credibility lost	2	Control over web platform (defacement)
Service impact	3	Successful response to unauthorised traffic
No service impact	4 (low)	Unsuccessful response to unauthorised traffic

Sensitive objects

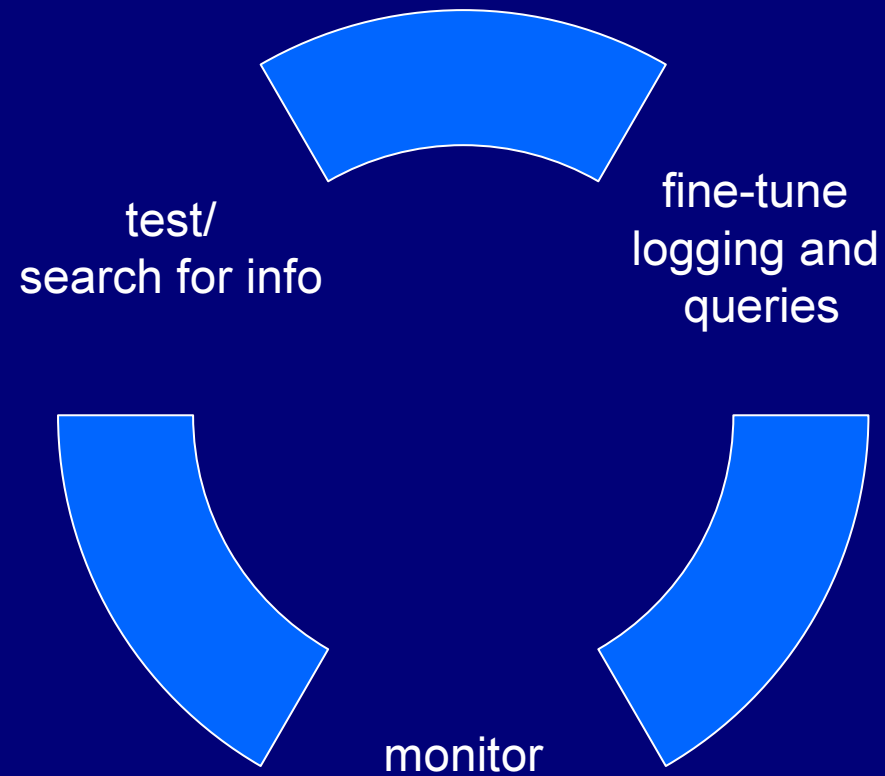
- E.g.
 - Client data
 - Intellectual property
 - Critical servers, network components
 - Security data
 - Services, tools
 - Information about the environment

Sixty-four thousand euro questions

Where to find relevant information?

How to translate these high-level questions and incident descriptions into queries ranging over low-level events found in a computer environment?

Sixty-four thousand euro answer



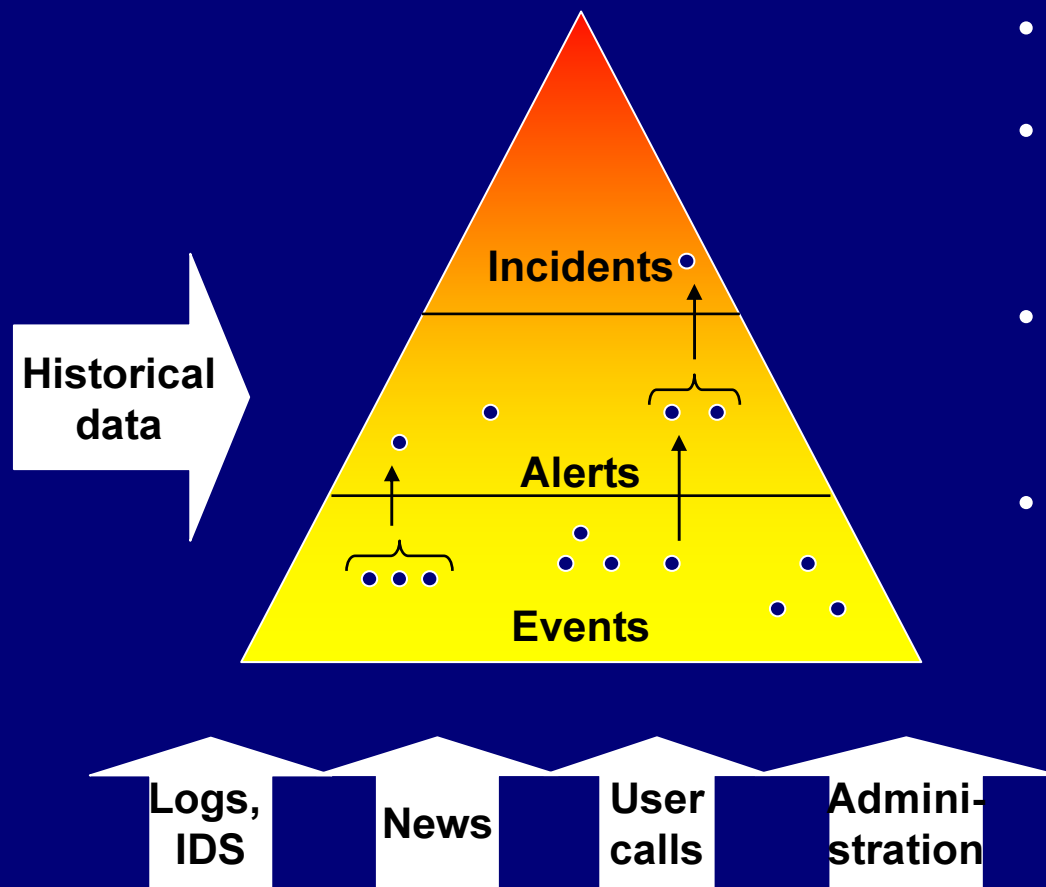
Sources of information

- information collected in the computer environment:
 - log files (OS, web platform, network components)
 - intrusion detection sensors
 - documentation on configuration (incl. software versions, patches installed)
- parties involved
 - system administration
 - users (help desk)
 - content developers
- information found on the Internet:
 - news groups
 - mailing lists
- information dispatched by vendors (software, hardware)
- security reports
 - security reviews
 - risk assessments

Translating questions: Event IDs, intrusion detection signatures, logs (examples)

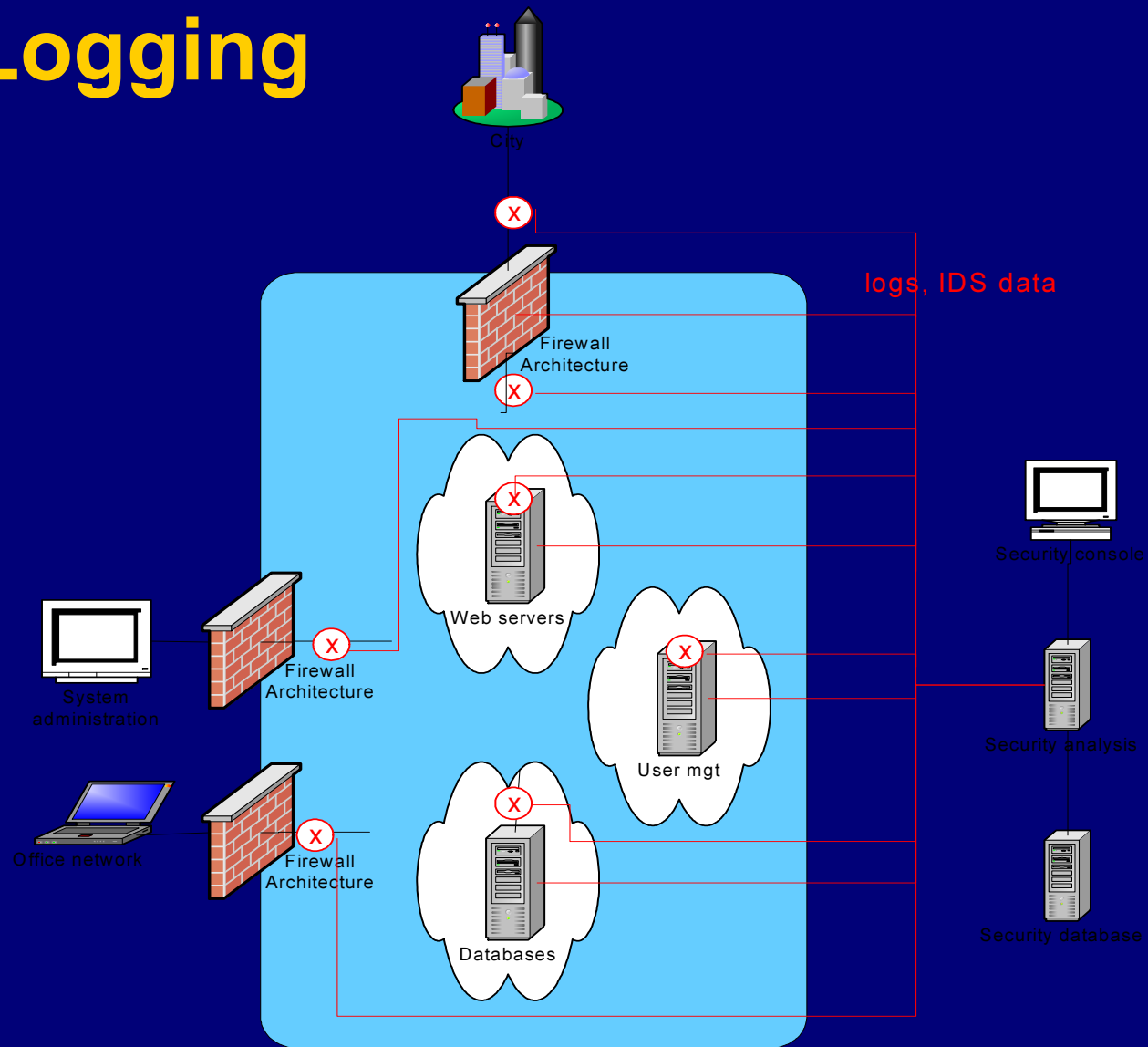
- Password cracking
 - e.g. Windows Event IDs:
 - 529 (log-on failure: wrong pw),
 - 644 (account lock-out)
 - 539 (log-on failure: account is locked out),
 - 528 (successful local log-on), 540 (successful network log-on)
- Windows executable attacks
 - corresponding intrusion detection signature,
or, .exe in web platform logs
 - look for responses in the web platform logs: e.g. 200(success) or 404(failure)

Translating questions: from events to incidents



- Define relevant sources
- Define expected relations between data
- Define incidents in terms of low-level events
- Decide what to display, what to store, and for which period of time

Logging



Monitoring

- important to detect incidents as early as possible:
 - automate checks/queries
 - identify the “normal behaviour” in order to be able to detect “abnormal behaviour”
- complexity of event analysis:
 - network size
 - separation of functionalities (database, web platform, user mgt, e-mail, browsing)
 - one action generates a series of low-level events on different components

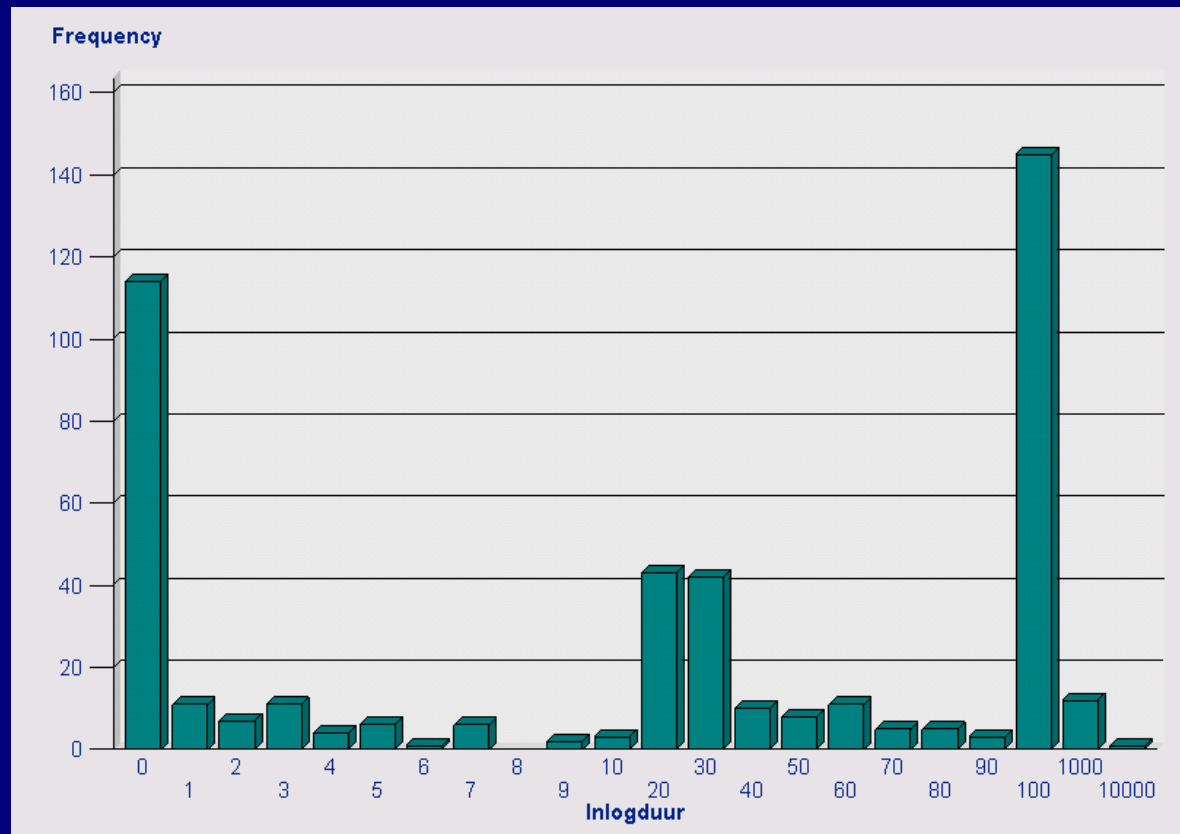
Monitoring: Intrusion detection

- host-based and network-based sensors
- network-based sensors:
 - inspecting packets for signatures of known attacks
 - three types of signatures: strings, ports or headers signatures
- host-based sensors: also OS events
- different questions for different network segments
- problems: (too) many false positives
- effective in response, although often unclear how traffic is analysed

Monitoring: Data analysis

- At Deloitte&Touche ERS:
data mining in security logs with the aim of
 - establishing “normal behaviour”
 - identifying/verifying correlations between events
 - scheduling checks, reducing the number of false positives, fine-tuning the logging
- Demo set up as follows:
 - in a Windows environment
 - log-on and log-off events (OS event IDs 528 resp. 538)
 - matching of log-ons and log-offs
 - database size: 2GB
 - tool for data analysis: SAS
 - statistics: averages, deviations, trends

Demo: Distribution of log-on periods



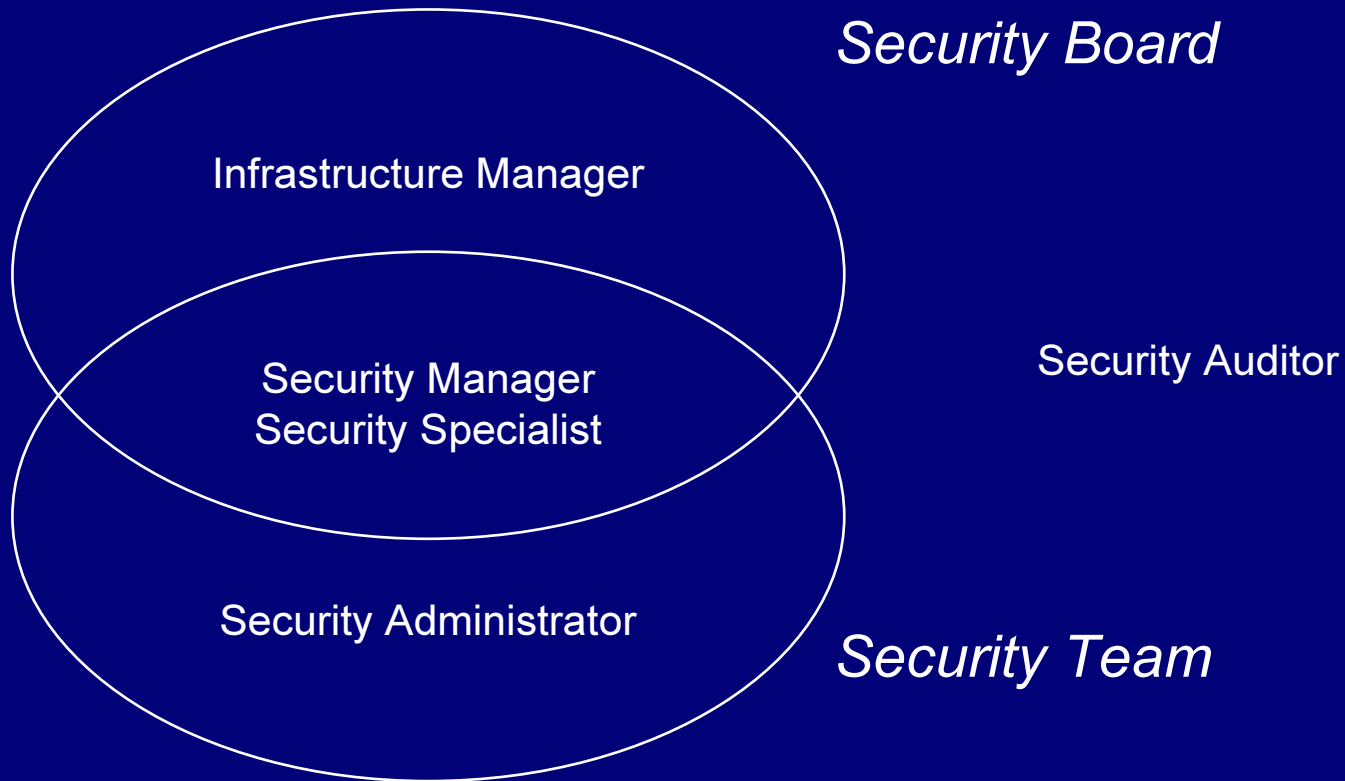
Reporting

- Regular reports on daily checks
- Trends and trends analysis
- Security tests: port scanners, network scanners, server scanners checking configuration of components, installed patches, weak passwords etc
- Security reviews: performed by auditors, more extensive than security tests, may include also operational procedures reviews, security policy reviews

Security of security monitoring?

- Protection of the security data
 - access to the data
 - security status of the security environment
- Security system administration:
 - backup
 - change management
 - patching etc
- Legal issues:
 - may the security data be collected?
 - warning banners to inform about monitoring

Roles in security monitoring



Security Team responsibilities

- setting up, maintaining the security policy
- ensuring adequate implementation of the security policy
- setting up security procedures
- ensuring adequate implementation of security procedures
- monitoring, analyzing and reporting
- setting up, maintaining security incident response procedures
- acting upon security incidents
- ensuring that an appropriate level of security is maintained

Security Board responsibilities

- reviewing, analyzing sec. reports and (disclosed) security incidents
- keeping up-to-date with major threats and taking action in case of (new) security breaches in a timely fashion
- assessing change requests
- advising on security-related improvements
- advising on the change and incident response procedures

Standards, guidelines, certificates

- ISO 17799 (a.k.a. BS7799)
- NoReA ZekeRE Business
- ITIL
- CoBiT
- SAS70
- Trust Services