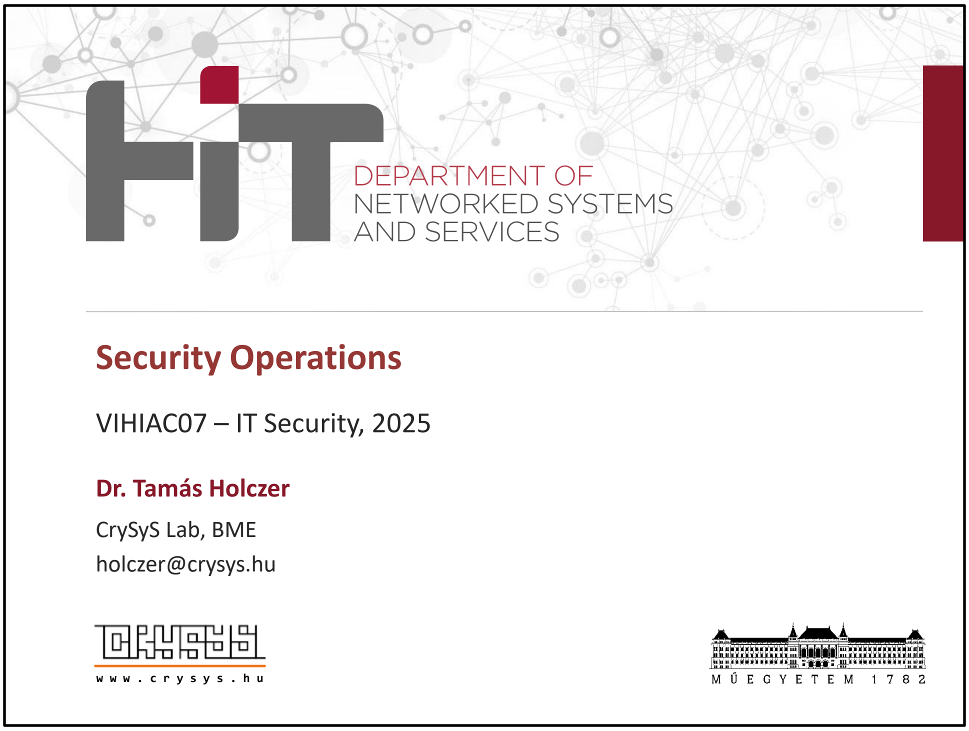


DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

# Security Operations

VIHIAC07 – IT Security, 2025

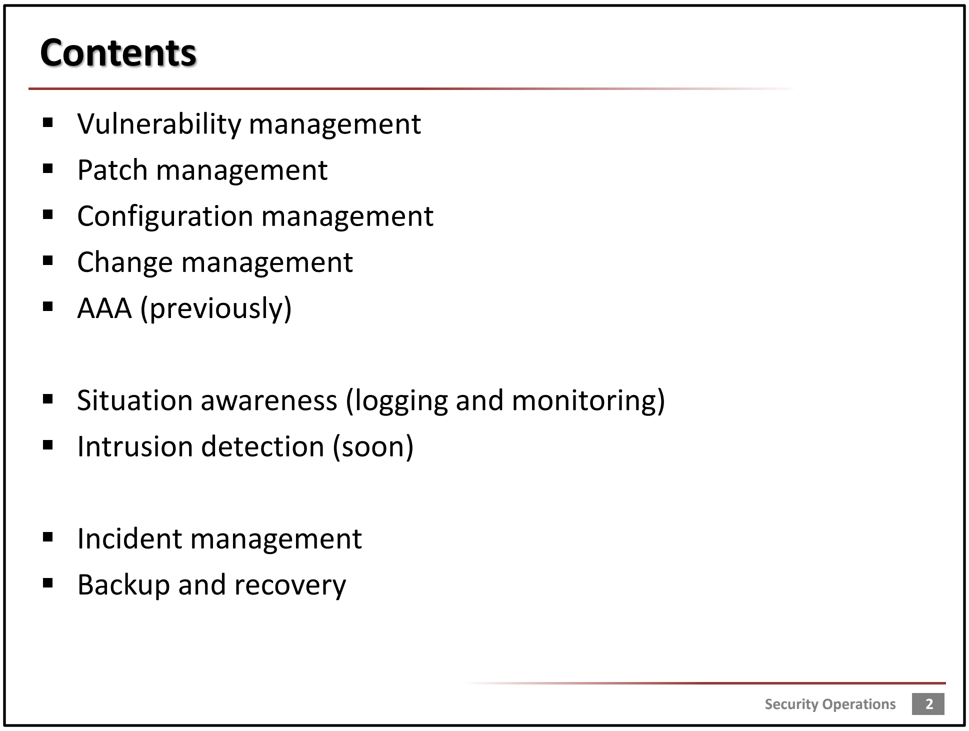
**Dr. Tamás Holczer**

CrySyS Lab, BME

holczer@crysys.hu

www.crysys.hu

MŰEGYETEM 1782



## Contents

- Vulnerability management
- Patch management
- Configuration management
- Change management
- AAA (previously)

- Situation awareness (logging and monitoring)
- Intrusion detection (soon)

- Incident management
- Backup and recovery

# PreDeCo - Ransomware

- Vulnerability management
- Patch management
- Cor
- Cha
- AA

Prevention

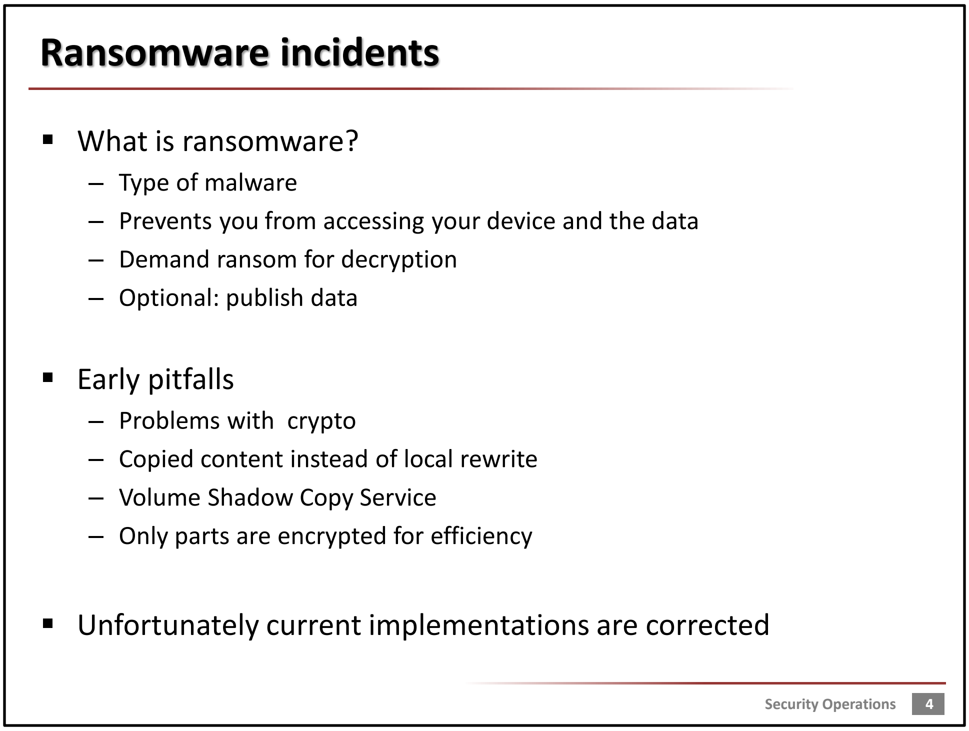
- Situ
- Int

Detection

- Inc
- Bac

Correction

Security is a pain in the *** in the short run but paying ransom is worse

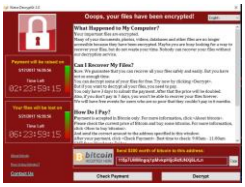


# Ransomware incidents

- What is ransomware?
  - Type of malware
  - Prevents you from accessing your device and the data
  - Demand ransom for decryption
  - Optional: publish data
- Early pitfalls
  - Problems with  crypto
  - Copied content instead of local rewrite
  - Volume Shadow Copy Service
  - Only parts are encrypted for efficiency
- Unfortunately current implementations are corrected

# Wannacry - 2017

- On Friday May 12th 2017, several organizations were affected by a new Ransomware strain.
- The Ransomware was very successful in part because it used a SMB vulnerability to spread inside networks.
- The vulnerability was patched by Microsoft in March for supported versions of Windows.
- The exploit, known under the name ETERNALBLUE, was released in April as part of a leak of NSA tools.
- Estimated > 200,000 victims according to various anti virus vendors in 150 countries
- Economic loss up to US$4 billion



Ooops, your files have been encrypted!

**What Happened to My Computer?**

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

[illegible]

Time Left

02:23:59:15

Your files will be lost on

[illegible]

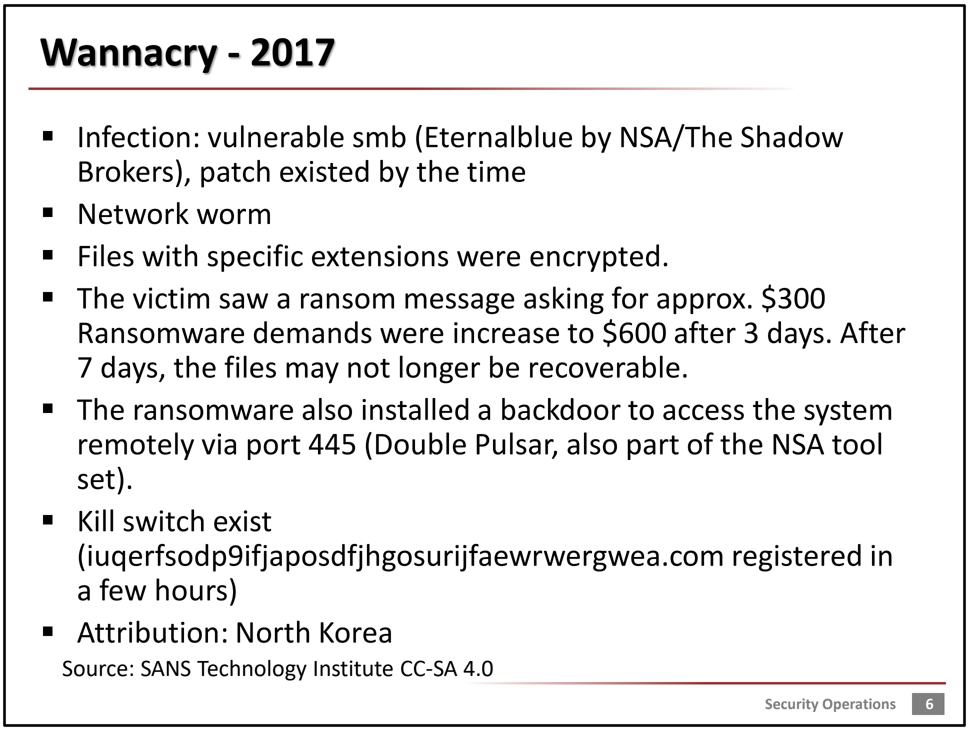
Time Left

06:23:59:15

Send $300 worth of bitcoin to this address:

[illegible]

Source: SANS Technology Institute CC-SA 4.0



## Wannacry - 2017

- Infection: vulnerable smb (Eternalblue by NSA/The Shadow Brokers), patch existed by the time
- Network worm
- Files with specific extensions were encrypted.
- The victim saw a ransom message asking for approx. $300 Ransomware demands were increase to $600 after 3 days. After 7 days, the files may not longer be recoverable.
- The ransomware also installed a backdoor to access the system remotely via port 445 (Double Pulsar, also part of the NSA tool set).
- Kill switch exist (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com registered in a few hours)
- Attribution: North Korea

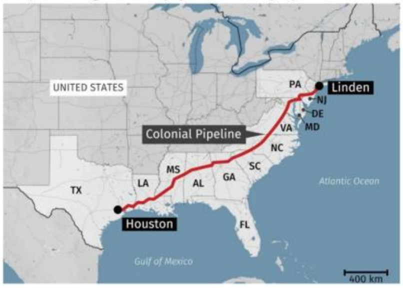
Source: SANS Technology Institute CC-SA 4.0

Eternalblue was stolen and leaked by The Shadow Brokers

# Colonial Pipeline attack - 2021

- Attackers used a compromised VPN password
- Targeted the billing system
- Ransom paid (75 bitcoin)
- 63.7 bitcoin recovered
- Pipelines restarted in 1 week

Major U.S. gasoline pipeline hit by cyberattack

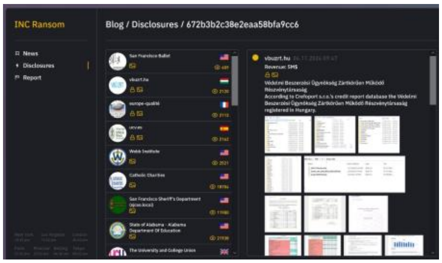


## Anyone can be a victim

- Synlab – Synnovis (hospital, operations cancelled, London), 2024
- Hipocrate Information System (hospitals central system, Romania), 2024
- UMC Health System (hospital, USA), 2024
- Sch KSzK, 2023
- CNEA Bariloche Atomic Center (Comision Nacional de Energia Atomica), 2024
- Védelmi Beszerzési Ügynökség

  2024
- Nemzeti Régészeti Intézet

  2025


INC Ransom
Blog / Disclosures / 672b3b2c38e2eaa58bfa9cc6
News
Disclosures
Report
San Francisco Ballet
vbuzrt.hu
europe-qualité
Webb Institute
Catholic Charities
San Francisco Sheriff's Department (sfgov.local)
State of Alabama - Alabama Department Of Education
The University and College Union

vbuzrt.hu

Revenue: 5M$

Védelmi Beszerzési Ügynökség Zártkörűen Működő Részvénytársaság

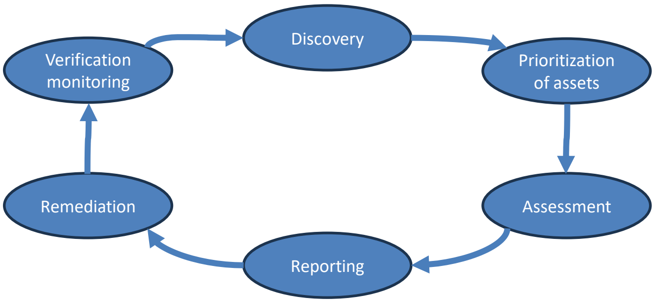
According to Creditport s.r.o.'s credit report database the Védelmi Beszerzési Ügynökség Zártkörűen Működő Részvénytársaság registered in Hungary.

[https://www.rionegro.com.ar/politica/hackearon-el-sistema-de-la-cnea-y-los-efectos-llegaron-al-centro-atomico-bariloche-3911600/](https://www.rionegro.com.ar/politica/hackearon-el-sistema-de-la-cnea-y-los-efectos-llegaron-al-centro-atomico-bariloche-3911600/)

## Prevention of security incidents

# Vulnerability management

- Continous proactive process (lifecycle)
- Reduce risk by minimizing exploitable vulnerabilities
- Why not patching all vulns?
  - Unknown vuln/asset
  - Limited manpower
  - Downtime restrictions



Discovery

Prioritization of assets

Assessment

Reporting

Remediation

Verification monitoring

# Vulnerability management

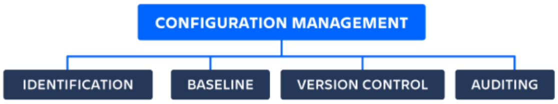
- Discovery
  - Create full asset inventory
  - Automatic vulnerability discovery
- Prioritize assets
  - How critical is the asset
  - How critical is the asset group (HA is against random failures)
- Assessment
  - Criticality of asset
  - Vulnerability classification
- Reporting
  - Create a mitigation plan
- Remediation
  - Fix the vulnerabilities with highest risk
- Update asset and vuln list (GOTO step 1)

# Patch management

- Part of vulnerability management
- Centralized process
- Apply vendor-issued patches (discovery might not find it yet)
- Remember: WannaCry used a patched well known SMB vuln
- Patch may contain
  - Security patch
  - Bug fixes
  - New features
- Patches must be prioritized
- Patches should be tested
- Related systems and admins must coordinate (downtime for others)
- Patch management is mandatory for compliance

# Configuration management

- Configuration must be managed of
  - Software assets
  - Operating system
  - Network devices
  - Hardware…
- Version control is generally used (git, svn, etc)
- Infrastructure as code
  - Terraform
  - Ansible, Salt Stack…
- Configuration should not be changed directly
- Auditing capabilities
- Helps recovery a lot



CONFIGURATION MANAGEMENT

IDENTIFICATION

BASELINE

VERSION CONTROL

AUDITING

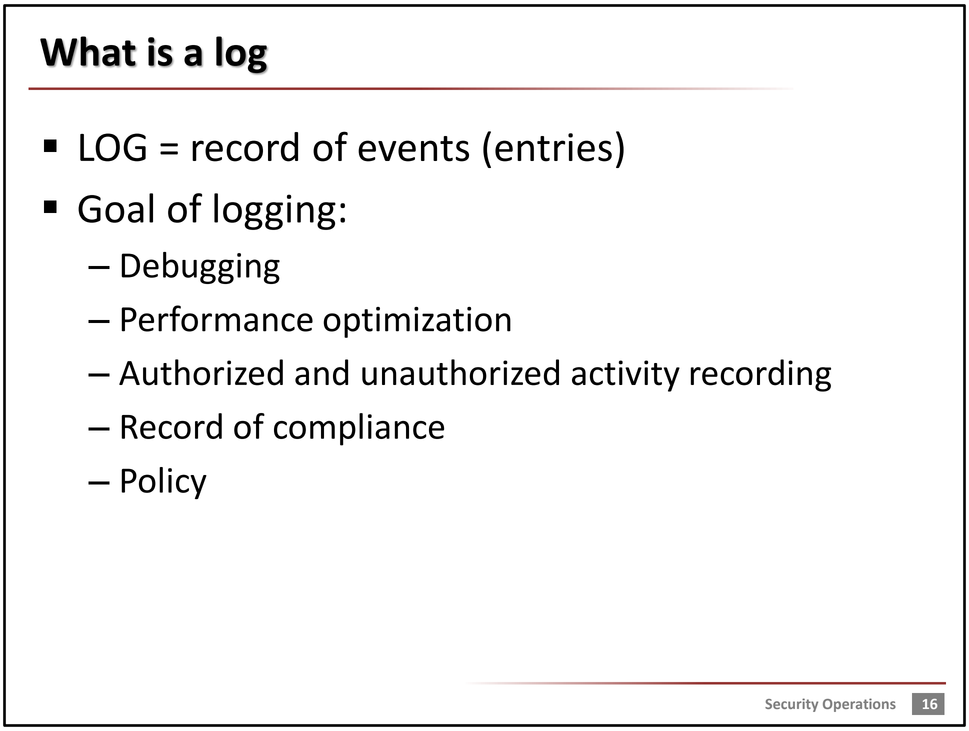
Image source: Atlassian

# Change management

- New systems and services are needed
  - Feature request
  - Support
  - Price
- Systems and services must be changed
- Select new candidates
- Evaluate candidates
- Design coexistence of systems
- Implement change
- Evaluation of change

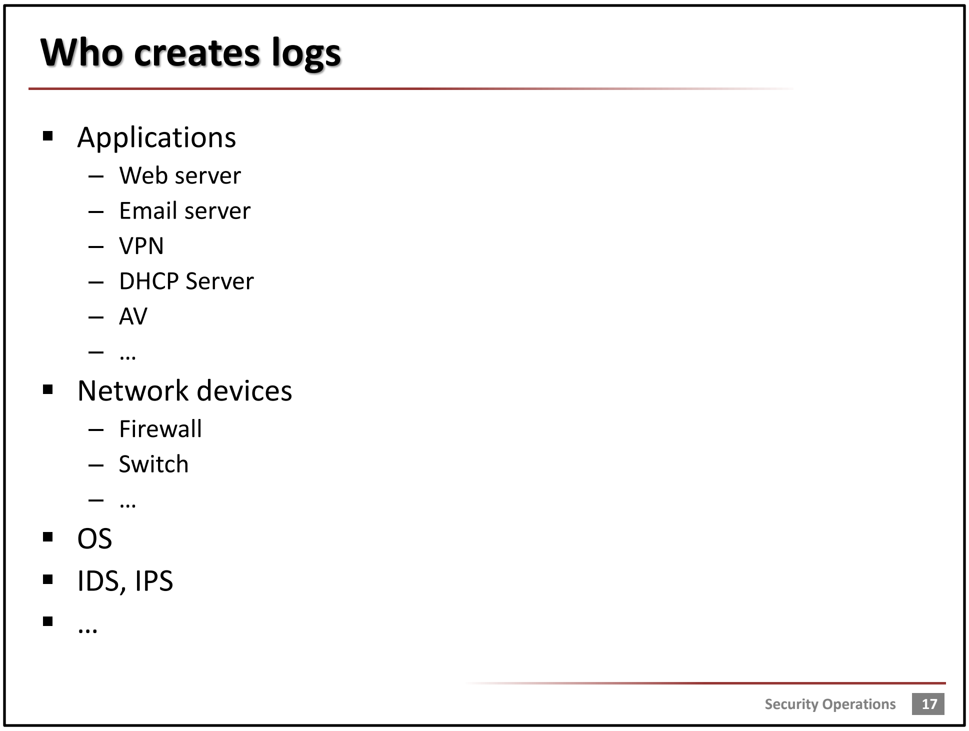
- Risk exposure may change

## Detection of security incidents



## What is a log

- LOG = record of events (entries)
- Goal of logging:
  - Debugging
  - Performance optimization
  - Authorized and unauthorized activity recording
  - Record of compliance
  - Policy

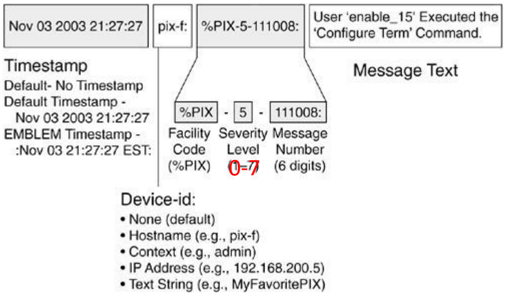


## Who creates logs

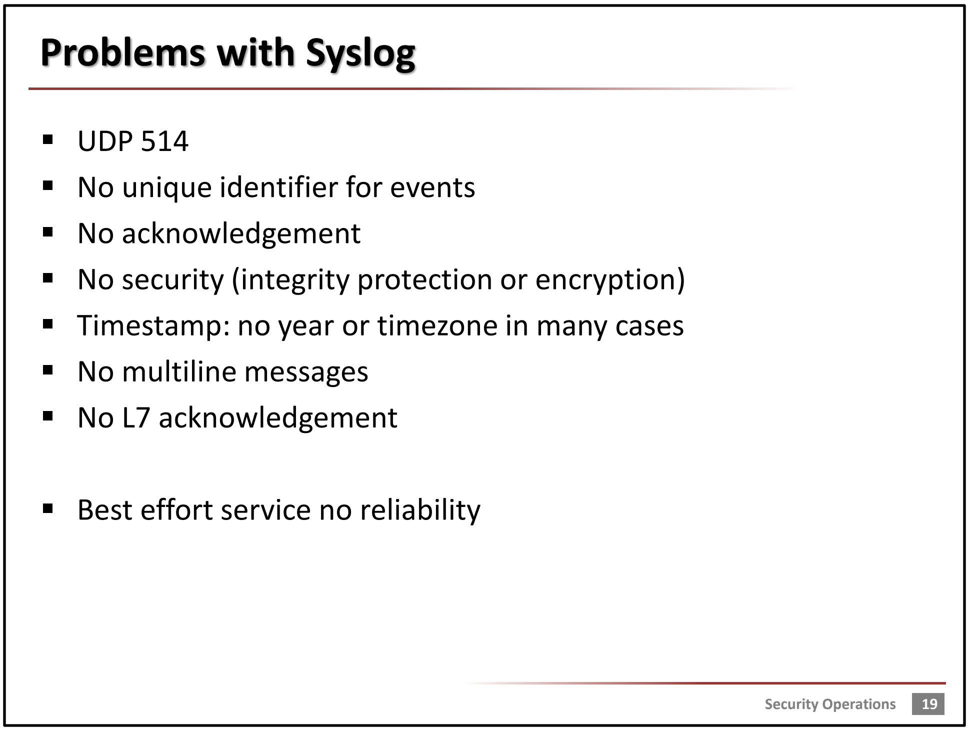
- Applications
  - Web server
  - Email server
  - VPN
  - DHCP Server
  - AV
  - …
- Network devices
  - Firewall
  - Switch
  - …
- OS
- IDS, IPS
- …

# BSD syslog (RFC3164)

- Developed in 80s
- Orig: part of sendmail
- RFC3164 2001
  - Documents the status
- RFC5424 2009
  - Standardizes syslog
  - Obsolotes 3164


Nov 03 2003 21:27:27
pix-f:
%PIX-5-111008:
User 'enable_15' Executed the 'Configure Term' Command.
Timestamp
Default- No Timestamp
Default Timestamp - Nov 03 2003 21:27:27
EMBLEM Timestamp - :Nov 03 21:27:27 EST:
Message Text
%PIX
5
111008:
Facility Code (%PIX)
Severity Level
0-7
Message Number (6 digits)
Device-id:
• None (default)
• Hostname (e.g., pix-f)
• Context (e.g., admin)
• IP Address (e.g., 192.168.200.5)
• Text String (e.g., MyFavoritePIX)

- Device ID: usually hostname (no FQDN)
- Facility: kern, user mail, daemon, auth…
- Severity: 0-Emergency, 7-Debug
- MSG: Latin-1 free text



## Problems with Syslog

- UDP 514
- No unique identifier for events
- No acknowledgement
- No security (integrity protection or encryption)
- Timestamp: no year or timezone in many cases
- No multiline messages
- No L7 acknowledgement

- Best effort service no reliability

## Syslog API and syslogd

- Applications normally uses the Syslog API
- Syslog events goes to /dev/log
- syslogd collects records from /dev/log and stores them (default: /var/log/syslog) according to a configuration

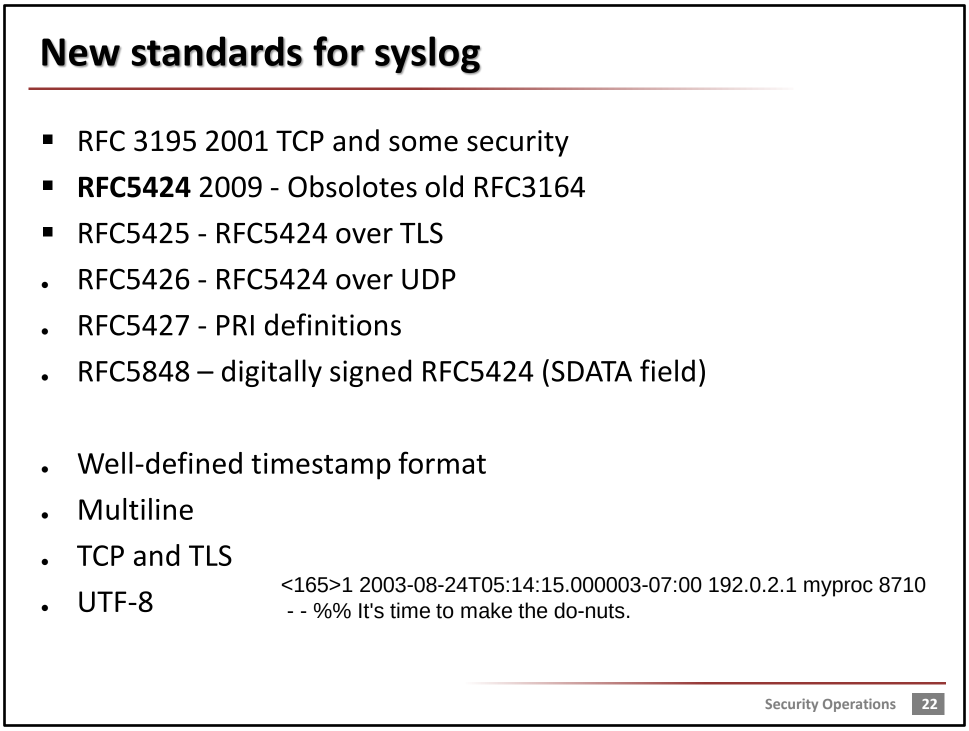
```
#include <syslog.h>
syslog (LOG_MAKEPRI(LOG_LOCAL1, LOG_ERROR), "Unable to make
network connection to %s.  Error=%m", host);
```

```
import syslog
syslog.syslog(syslog.LOG_ERR, ”Some error happened”)
```

# Reliable Delivery for syslog (RFC 3195 2001)

- Based on original RFC3164
- Uses TCP (acknowledgement)
- Cryptographic protectin
  - Encryption: TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - Authentication: based on MD5
- Raw profile: single line
- Cooked profile: multiline, xml

- Error codes from HTTP:
  - 200 Success
  - 500 General syntax error
  - …

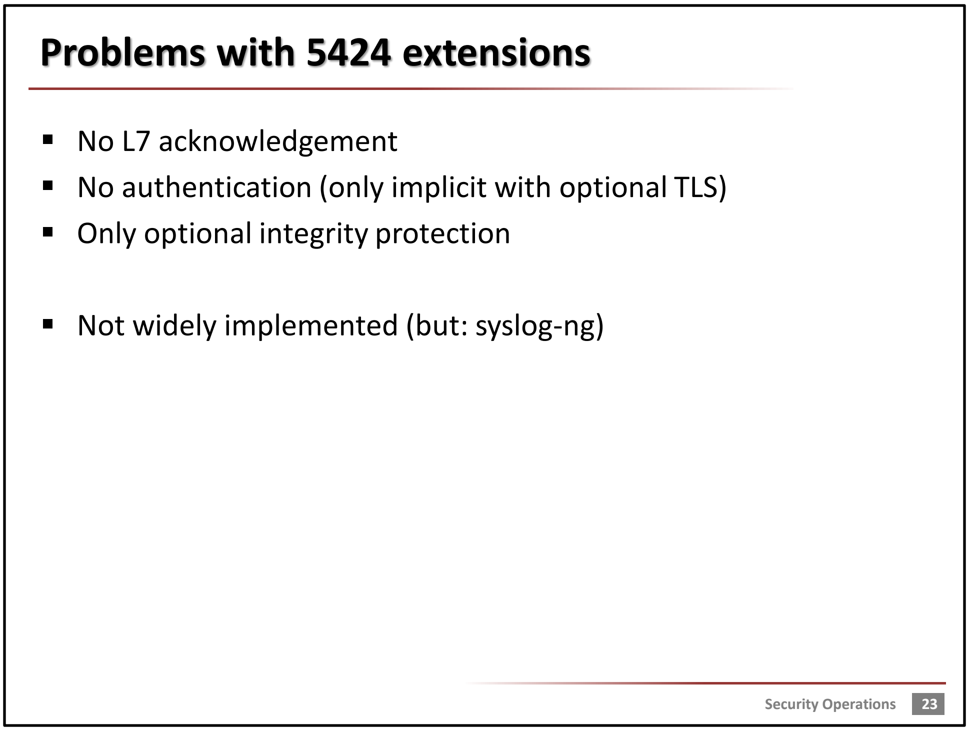


## New standards for syslog

- RFC 3195 2001 TCP and some security
- **RFC5424** 2009 - Obsolotes old RFC3164
- RFC5425 - RFC5424 over TLS
- RFC5426 - RFC5424 over UDP
- RFC5427 - PRI definitions
- RFC5848 – digitally signed RFC5424 (SDATA field)

- Well-defined timestamp format
- Multiline
- TCP and TLS
- UTF-8

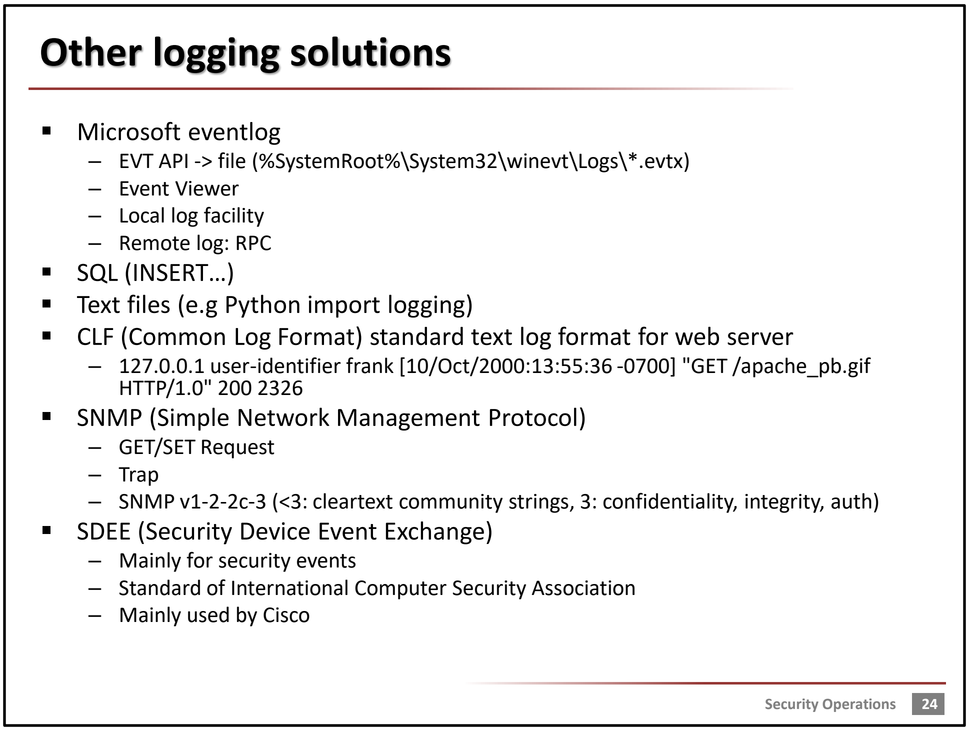
```
<165>1 2003-08-24T05:14:15.000003-07:00 192.0.2.1 myproc 8710
 - - %% It's time to make the do-nuts.
```



## Problems with 5424 extensions

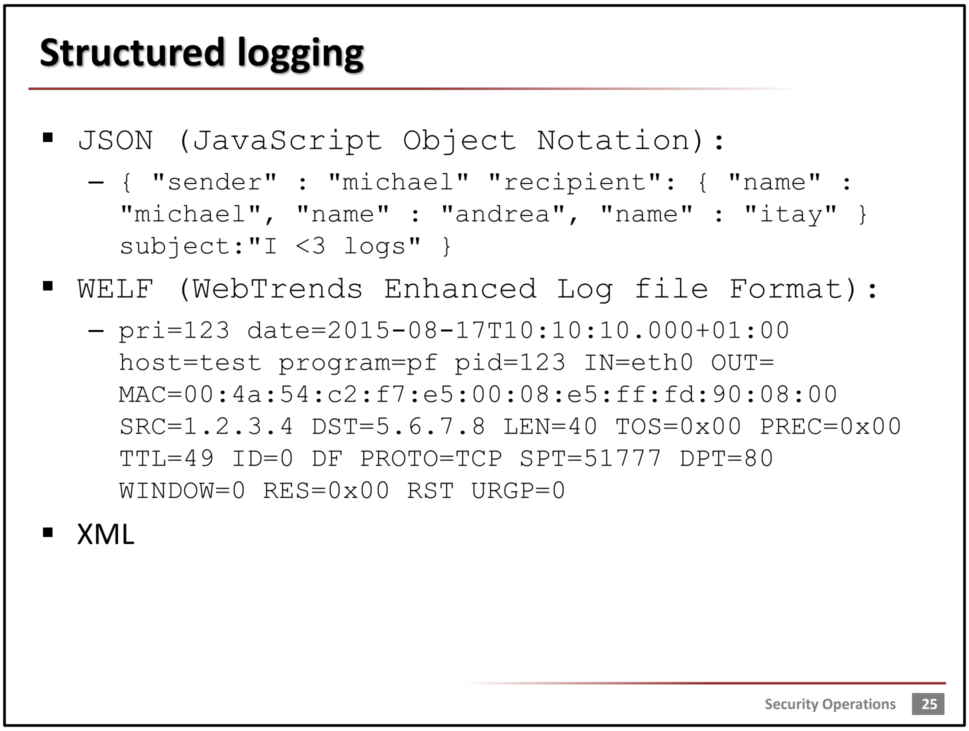
- No L7 acknowledgement
- No authentication (only implicit with optional TLS)
- Only optional integrity protection

- Not widely implemented (but: syslog-ng)



# Other logging solutions

- Microsoft eventlog
  - EVT API -> file (%SystemRoot%\System32\winevt\Logs\*.evtx)
  - Event Viewer
  - Local log facility
  - Remote log: RPC
- SQL (INSERT…)
- Text files (e.g Python import logging)
- CLF (Common Log Format) standard text log format for web server
  - 127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
- SNMP (Simple Network Management Protocol)
  - GET/SET Request
  - Trap
  - SNMP v1-2-2c-3 (<3: cleartext community strings, 3: confidentiality, integrity, auth)
- SDEE (Security Device Event Exchange)
  - Mainly for security events
  - Standard of International Computer Security Association
  - Mainly used by Cisco

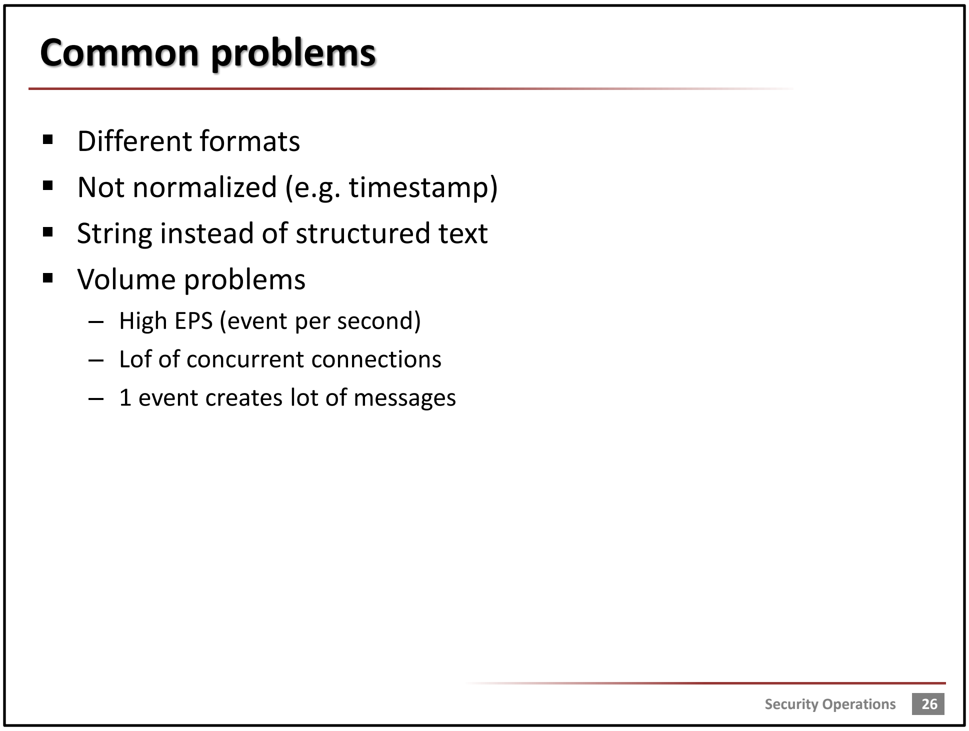


## Structured logging

- JSON (JavaScript Object Notation):

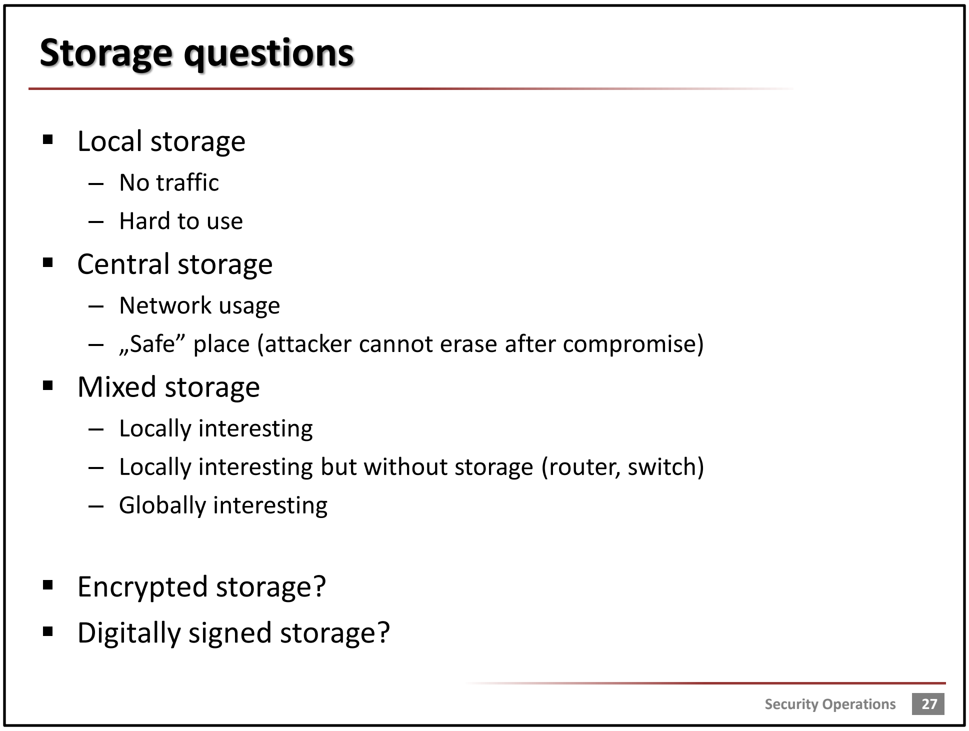
  -
    ```
    { "sender" : "michael" "recipient": { "name" :
    "michael", "name" : "andrea", "name" : "itay" }
    subject:"I <3 logs" }
    ```
- WELF (WebTrends Enhanced Log file Format):

  -
    ```
    pri=123 date=2015-08-17T10:10:10.000+01:00
    host=test program=pf pid=123 IN=eth0 OUT=
    MAC=00:4a:54:c2:f7:e5:00:08:e5:ff:fd:90:08:00
    SRC=1.2.3.4 DST=5.6.7.8 LEN=40 TOS=0x00 PREC=0x00
    TTL=49 ID=0 DF PROTO=TCP SPT=51777 DPT=80
    WINDOW=0 RES=0x00 RST URGP=0
    ```
- XML



## Common problems

- Different formats
- Not normalized (e.g. timestamp)
- String instead of structured text
- Volume problems
  - High EPS (event per second)
  - Lof of concurrent connections
  - 1 event creates lot of messages



# Storage questions

- Local storage
  - No traffic
  - Hard to use
- Central storage
  - Network usage
  - „Safe” place (attacker cannot erase after compromise)
- Mixed storage
  - Locally interesting
  - Locally interesting but without storage (router, switch)
  - Globally interesting

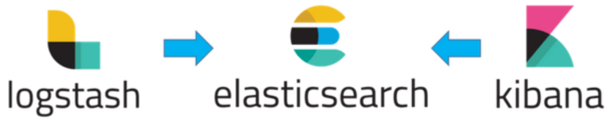
- Encrypted storage?
- Digitally signed storage?

# Packet capture

- Full packet capture (mainly for forensics, later in this lecture)
- Flow collection
  - Who communicates with whom at when
  - No payload collected
  - NetFlow / IPFIX (NetFlow v10)
  - Source IP, Destination IP, Source port, Destination port, Time, Header fileds…
  - Sender: router, switch, firewall, server…
  - Destination: flow collector
  - Analyser: dashboard, report, alert

Name
New York Core Router
Current Address
172.16.0.127
Description
Discovered as a NetFlow exporter

## The ELK Stack

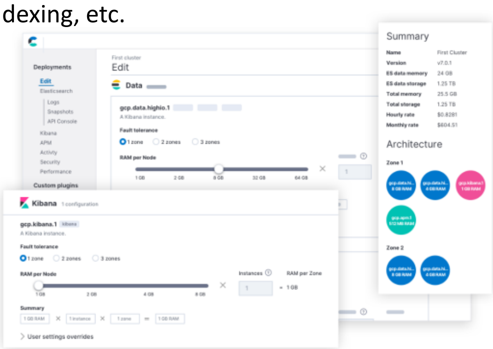


- ELK = elasticsearch, logstash, kibana

- One of the most popular log management and analytics solutions
- All open source software

# The ELK Stack

- Elasticsearch
  - A search and analytics engine, based on Apache Lucene
  - A NoSQL database
  - Has a REST API
  - Sharding and replica support
  - Plugins for analysis, alerting, indexing, etc.
  - Written in Java

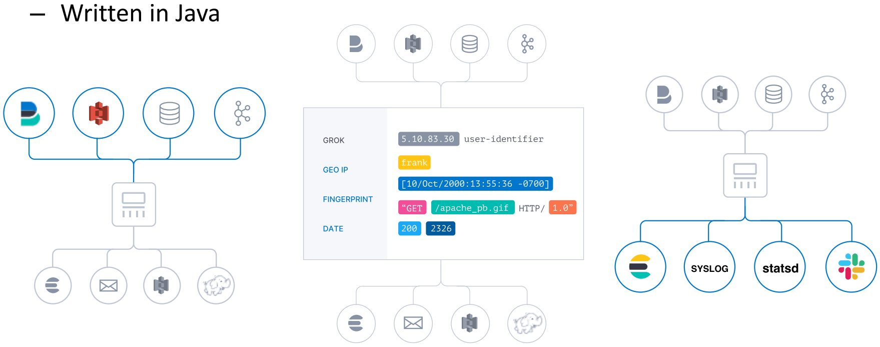


Summary

| | |
|---|---|
| Name | First Cluster |
| Version | v7.0.1 |
| ES data memory | 24 GB |
| ES data storage | 1.25 TB |
| Total memory | 25.5 GB |
| Total storage | 1.25 TB |
| Hourly rate | $0.8281 |
| Monthly rate | $604.51 |

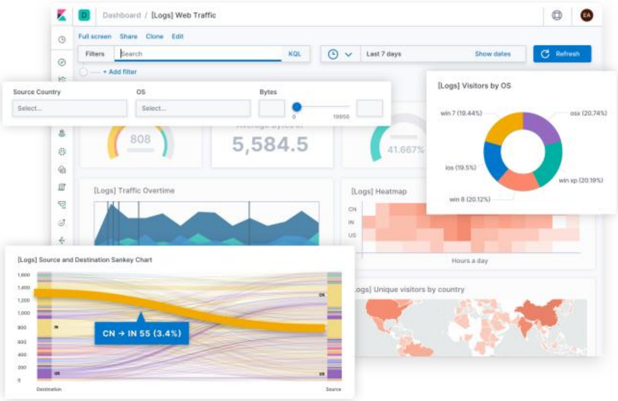
# The ELK Stack

- Logstash (Alternative: Fluentd/td-agent)
  - Collects and processes logs from different sources
  - Supports more than 50 different source formats
  - Supports several output formats
  - In our case, it feeds data to Elasticsearch
  - Written in Java



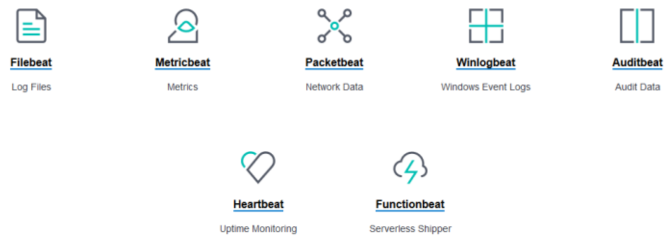
# The ELK Stack

- Kibana
  - A web interface to query data in Elasticsearch
  - Data visualization, dashboards
  - Written in node.js

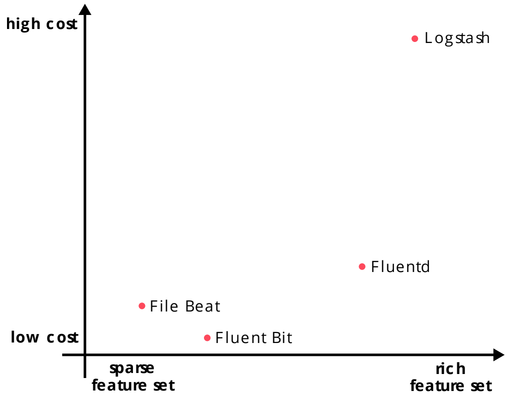


# The ELK Stack

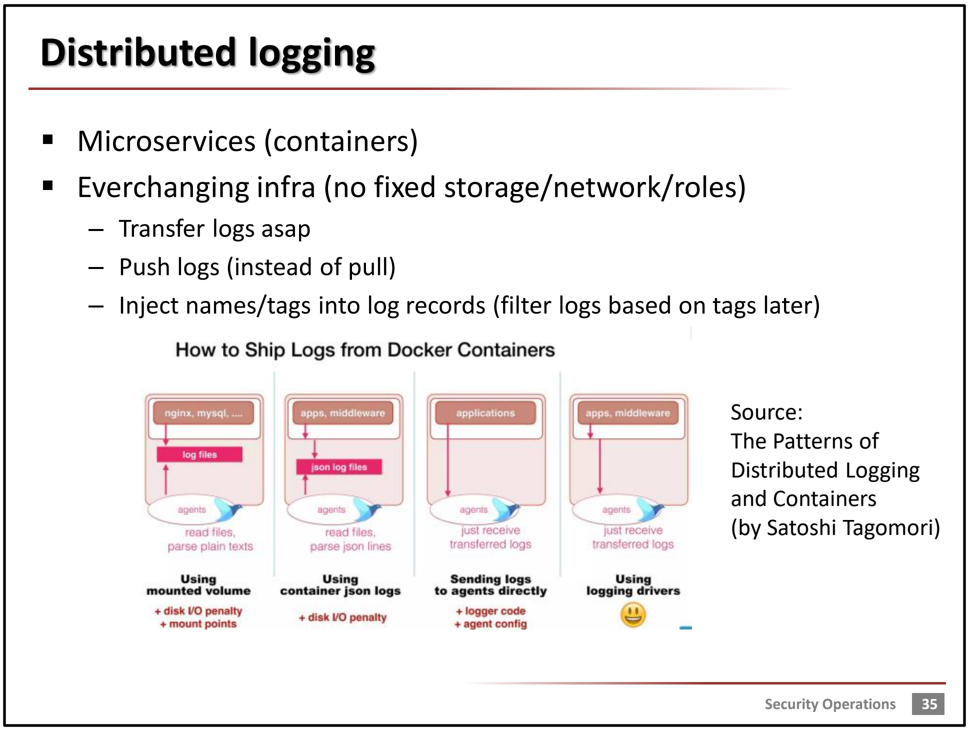
- Beats (Alternative: Fluentbit)
  - Originally not part of the ELK stack
  - Collects and feeds extra information (not necessarily logs)
  - Written in Go



# Logstash vs Beats vs Fluentd vs Fluentbit



Source: velebit.ai



# Distributed logging

- Microservices (containers)
- Everchanging infra (no fixed storage/network/roles)
  - Transfer logs asap
  - Push logs (instead of pull)
  - Inject names/tags into log records (filter logs based on tags later)

How to Ship Logs from Docker Containers

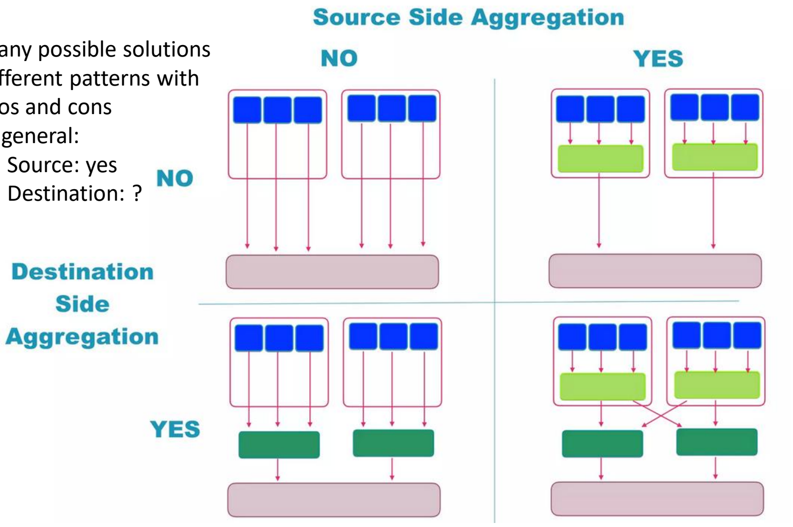
Source:
The Patterns of Distributed Logging and Containers
(by Satoshi Tagomori)

https://www.slideshare.net/tagomoris/the-patterns-of-distributed-logging-and-containers

# Where to aggregate?

Many possible solutions
Different patterns with pros and cons
In general:

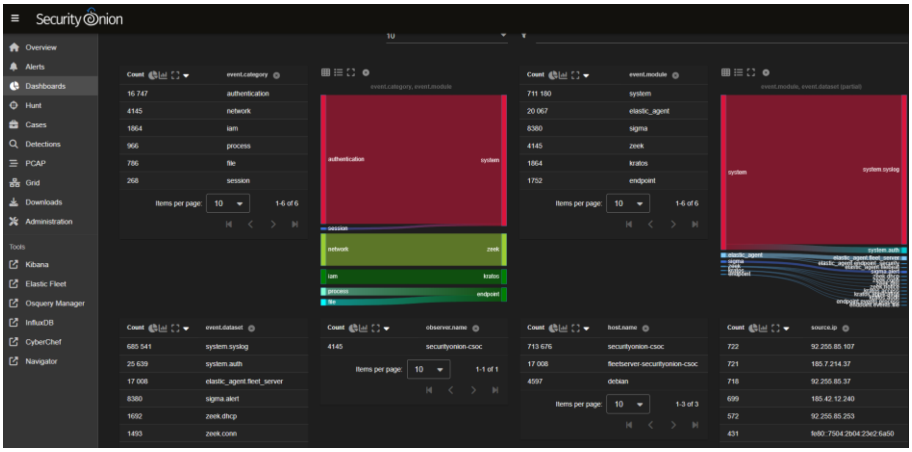
- Source: yes
- Destination: ?



Source: The Patterns of Distributed Logging and Containers (by Satoshi Tagomori)

# SIEM

- To be discussed soon



| Count | event.category |
|---|---|
| 16 747 | authentication |
| 4145 | network |
| 1864 | iam |
| 966 | process |
| 786 | file |
| 268 | session |

Items per page: 10 1-6 of 6

| Count | event.module |
|---|---|
| 711 180 | system |
| 20 067 | elastic_agent |
| 8380 | sigma |
| 4145 | zeek |
| 1864 | kratos |
| 1752 | endpoint |

Items per page: 10 1-6 of 6

| Count | event.dataset |
|---|---|
| 685 541 | system.syslog |
| 25 639 | system.auth |
| 17 008 | elastic_agent.fleet_server |
| 8380 | sigma.alert |
| 1692 | zeek.dhcp |
| 1493 | zeek.conn |

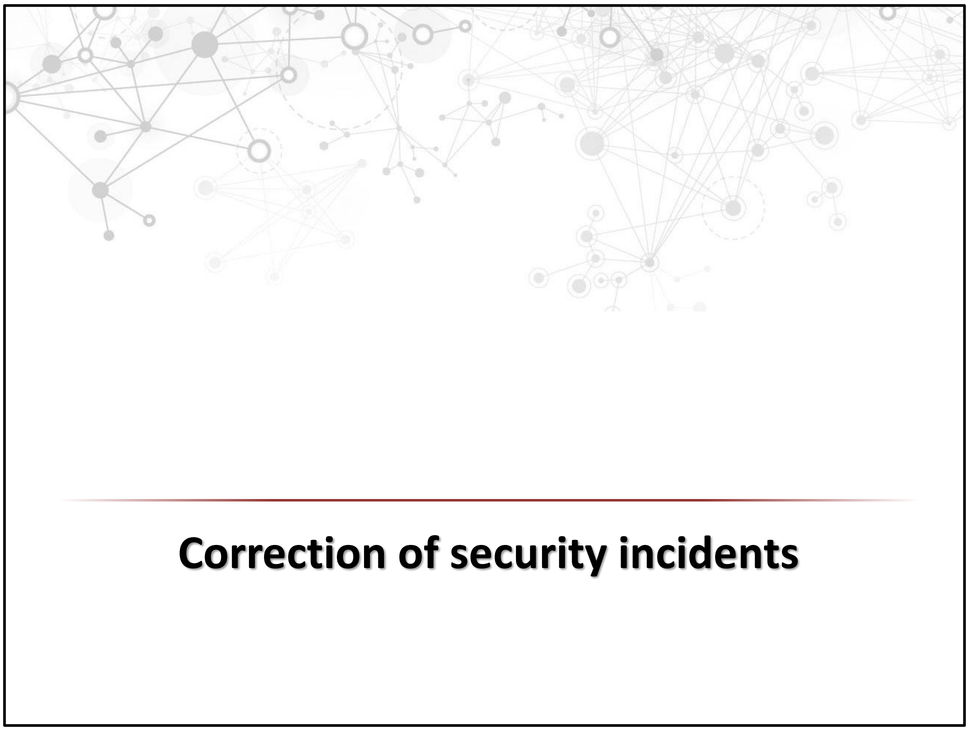
| Count | observer.name |
|---|---|
| 4145 | securityonion-csoc |

Items per page: 10 1-1 of 1

| Count | host.name |
|---|---|
| 713 676 | securityonion-csoc |
| 17 008 | fleetserver-securityonion-csoc |
| 4597 | debian |

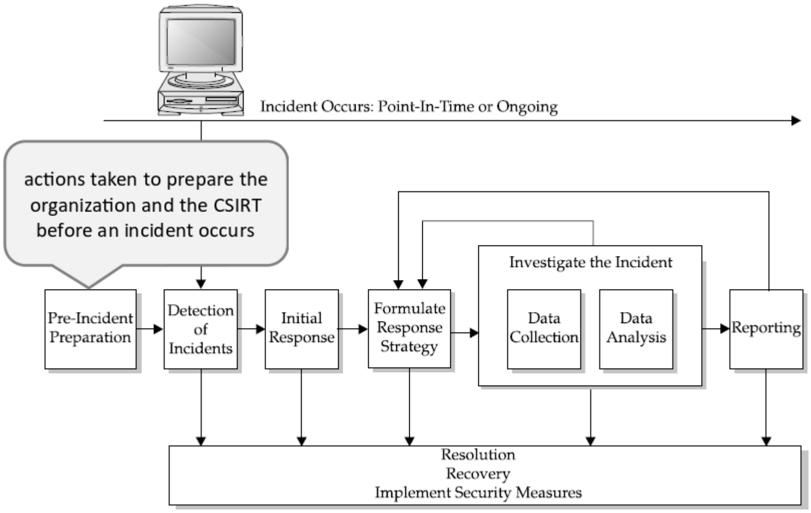
Items per page: 10 1-3 of 3

| Count | source.ip |
|---|---|
| 722 | 92.255.85.107 |
| 721 | 185.7.214.37 |
| 718 | 92.255.85.37 |
| 699 | 185.42.12.240 |
| 572 | 92.255.85.253 |
| 431 | fe80::7504:2b04:23e2:6a50 |



# Correction of security incidents

# Incident management



Incident Occurs: Point-In-Time or Ongoing

actions taken to prepare the organization and the CSIRT before an incident occurs

Pre-Incident Preparation

Detection of Incidents

Initial Response

Formulate Response Strategy

Investigate the Incident

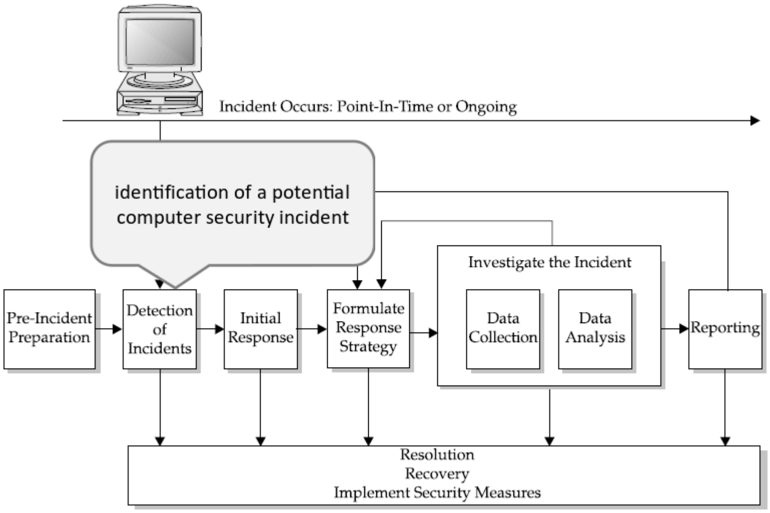
Data Collection

Data Analysis

Reporting

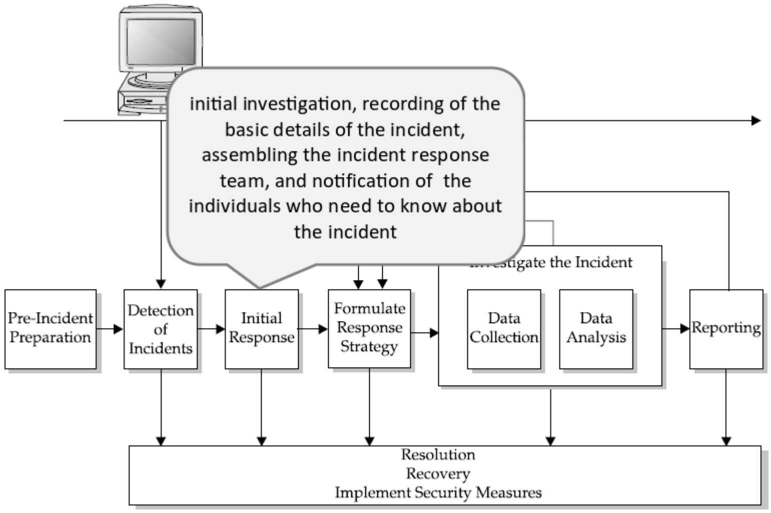
Resolution
Recovery
Implement Security Measures

# Incident management



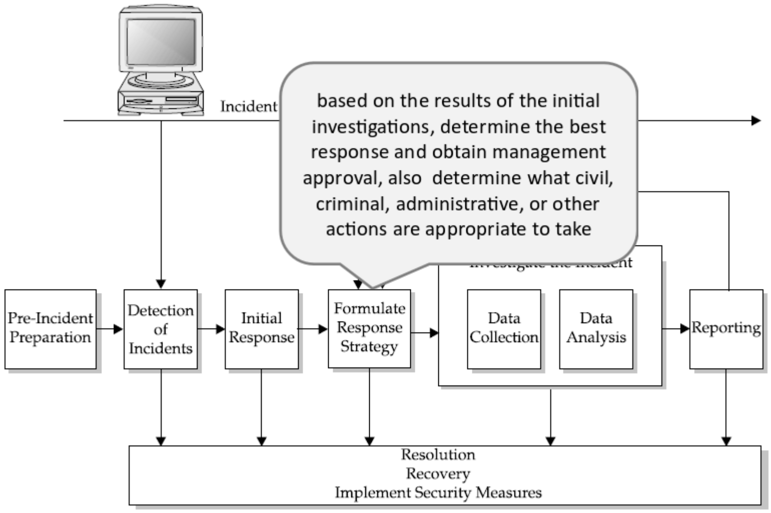
identification of a potential computer security incident

# Incident management



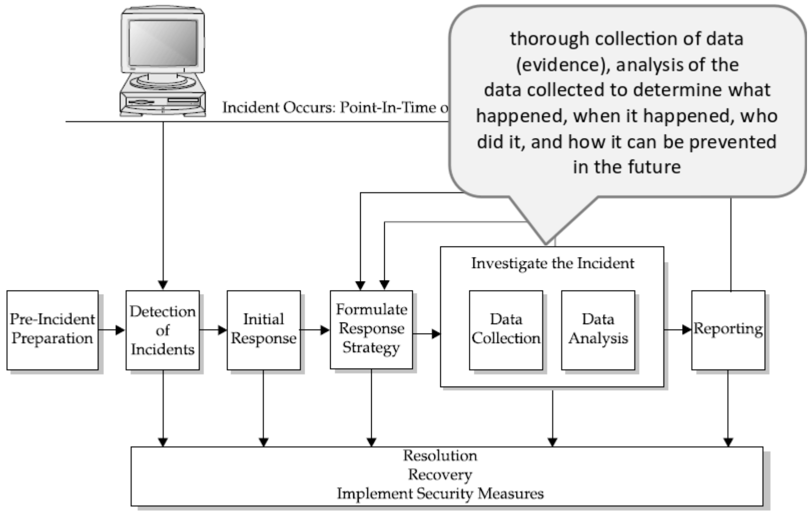
initial investigation, recording of the basic details of the incident, assembling the incident response team, and notification of the individuals who need to know about the incident

# Incident management



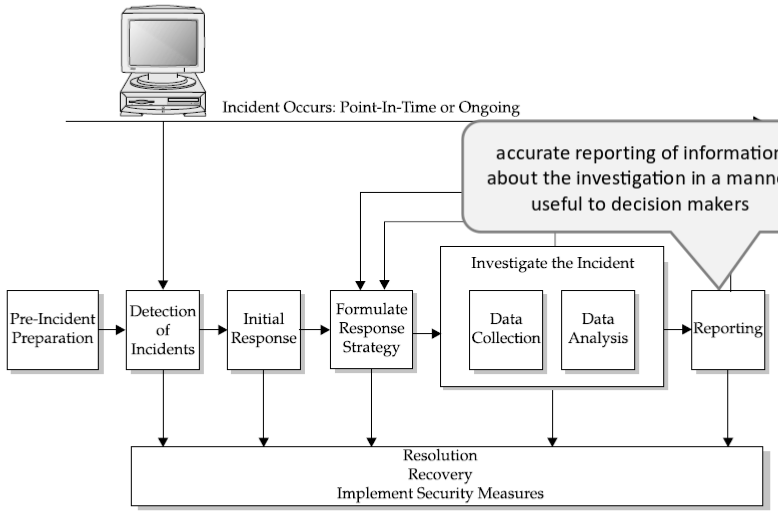
based on the results of the initial investigations, determine the best response and obtain management approval, also determine what civil, criminal, administrative, or other actions are appropriate to take

# Incident management



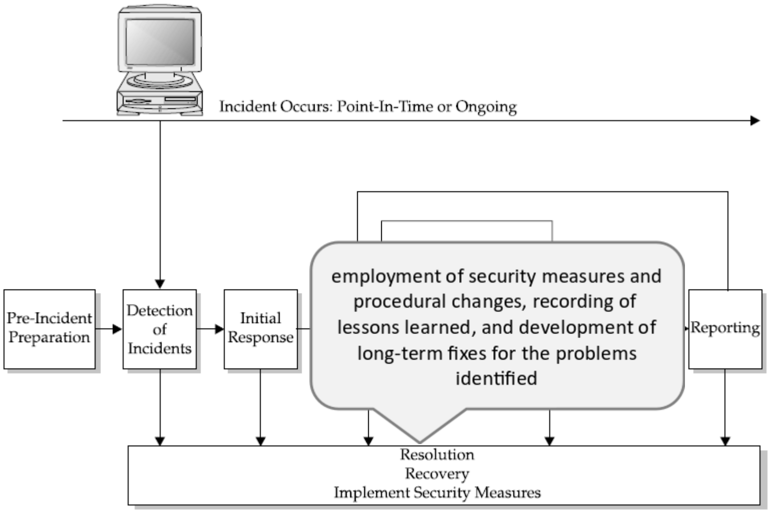
thorough collection of data (evidence), analysis of the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future

# Incident management

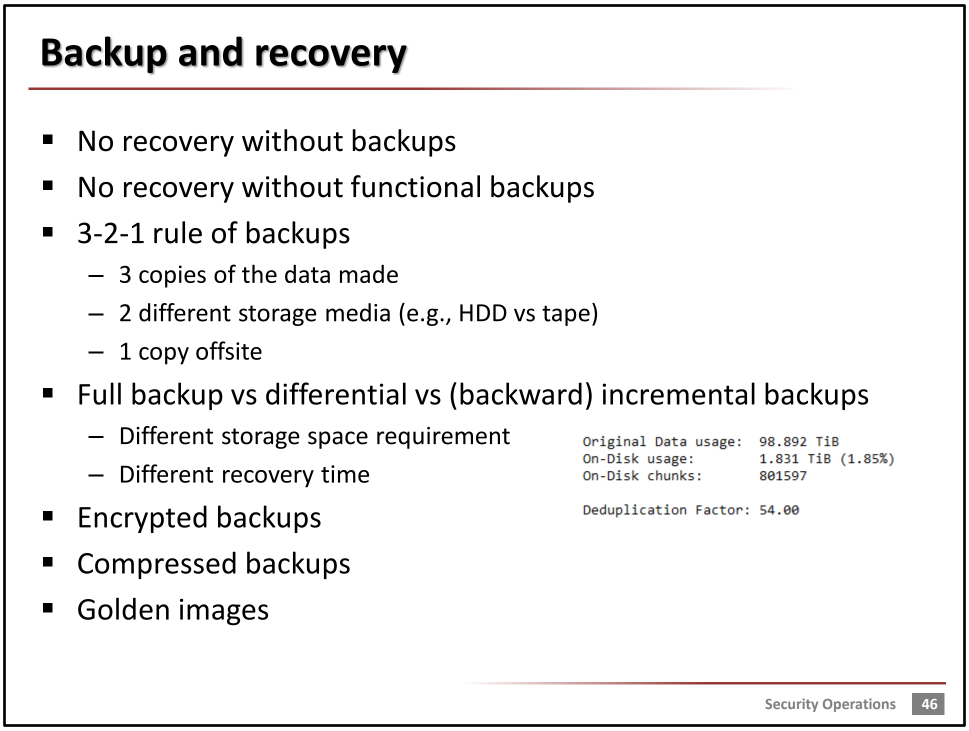


accurate reporting of information about the investigation in a manner useful to decision makers

# Incident management



employment of security measures and procedural changes, recording of lessons learned, and development of long-term fixes for the problems identified

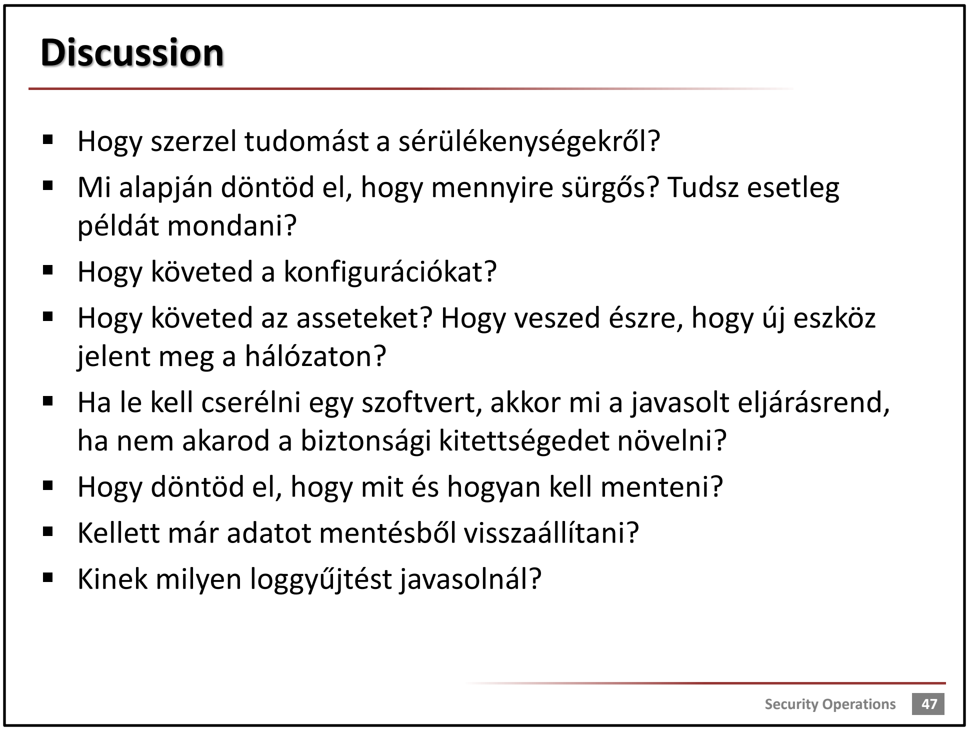


## Backup and recovery

- No recovery without backups
- No recovery without functional backups
- 3-2-1 rule of backups
  - 3 copies of the data made
  - 2 different storage media (e.g., HDD vs tape)
  - 1 copy offsite
- Full backup vs differential vs (backward) incremental backups
  - Different storage space requirement
  - Different recovery time
- Encrypted backups
- Compressed backups
- Golden images

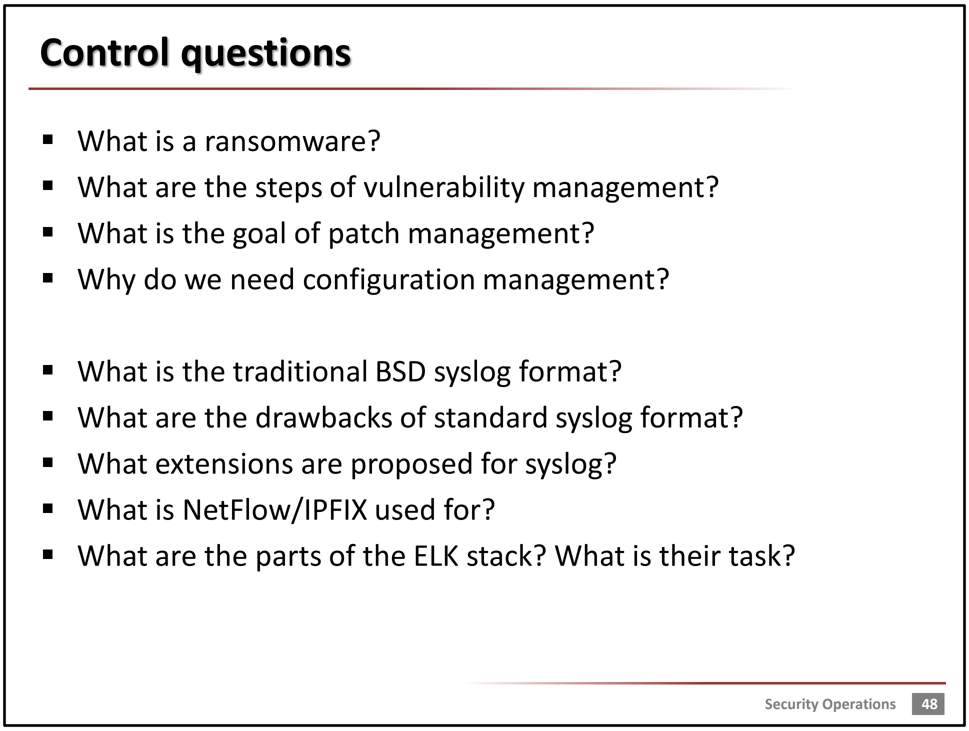
```
Original Data usage:  98.892 TiB
On-Disk usage:        1.831 TiB (1.85%)
On-Disk chunks:       801597

Deduplication Factor: 54.00
```

Differential: change since last full
Incremental: change since last backup



## Discussion

- Hogy szerzel tudomást a sérülékenységekről?
- Mi alapján döntöd el, hogy mennyire sürgős? Tudsz esetleg példát mondani?
- Hogy követed a konfigurációkat?
- Hogy követed az asseteket? Hogy veszed észre, hogy új eszköz jelent meg a hálózaton?
- Ha le kell cserélni egy szoftvert, akkor mi a javasolt eljárásrend, ha nem akarod a biztonsági kitettségedet növelni?
- Hogy döntöd el, hogy mit és hogyan kell menteni?
- Kellett már adatot mentésből visszaállítani?
- Kinek milyen loggyűjtést javasolnál?



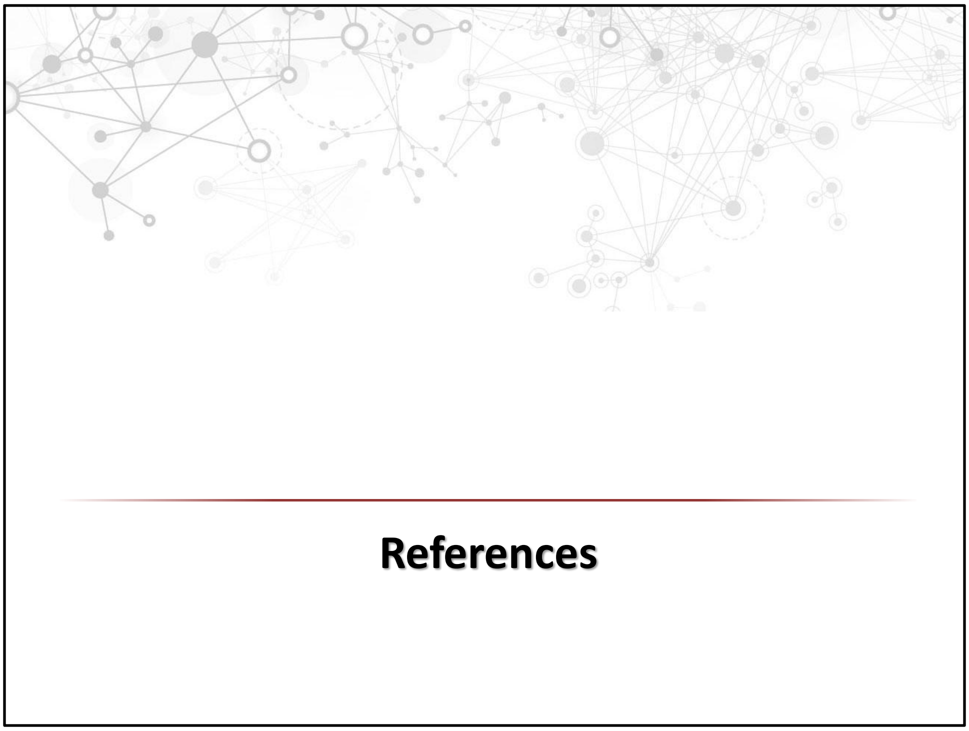
## Control questions

- What is a ransomware?
- What are the steps of vulnerability management?
- What is the goal of patch management?
- Why do we need configuration management?

- What is the traditional BSD syslog format?
- What are the drawbacks of standard syslog format?
- What extensions are proposed for syslog?
- What is NetFlow/IPFIX used for?
- What are the parts of the ELK stack? What is their task?

# Control Questions

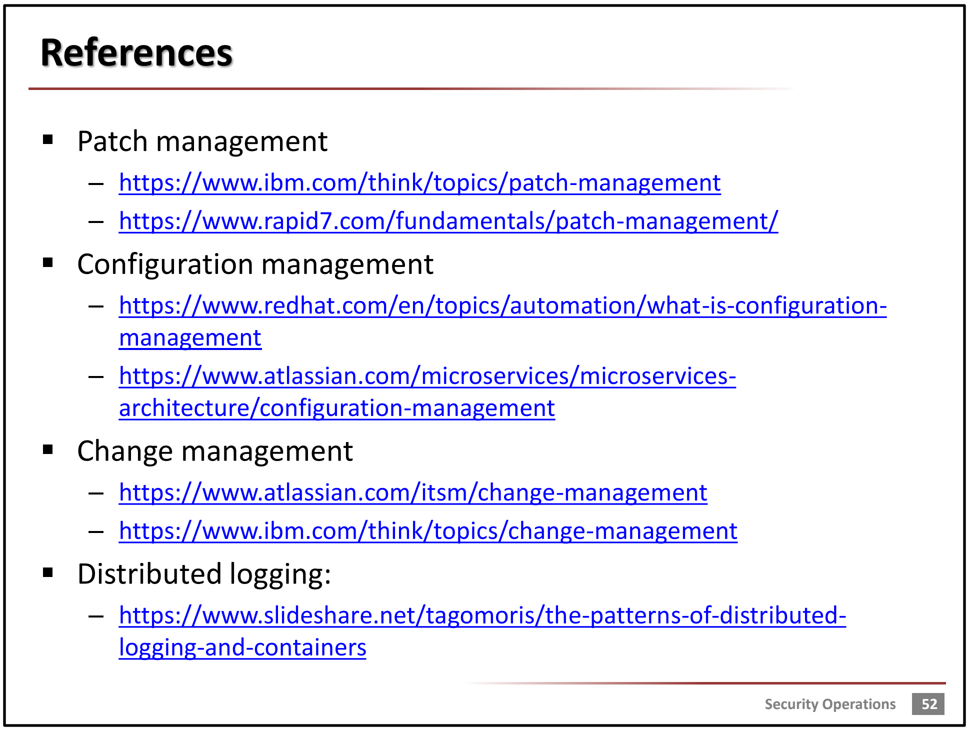
- What are the steps of incident management?
- Why do we need backup
- What kind of backup strategies do you know
- What is the 3-2-1 rule in backuping?



# References

# References

- CyBok Security Operations & Incident Management
  - https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf
- WannaCry
  - https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
  - https://www.sans.org/blog/wannacry-wannacrypt-ransomware-resources/
- Vulnerability management
  - https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management
  - https://www.ibm.com/think/topics/vulnerability-management



# References

- Patch management
  - https://www.ibm.com/think/topics/patch-management
  - https://www.rapid7.com/fundamentals/patch-management/
- Configuration management
  - https://www.redhat.com/en/topics/automation/what-is-configuration-management
  - https://www.atlassian.com/microservices/microservices-architecture/configuration-management
- Change management
  - https://www.atlassian.com/itsm/change-management
  - https://www.ibm.com/think/topics/change-management
- Distributed logging:
  - https://www.slideshare.net/tagomoris/the-patterns-of-distributed-logging-and-containers