# Introduction – what, why, how

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Security of IT infrastructure (2023/24)

# Content

What could go wrong – few examples

Vulnerabilities, classifications

Real world

- Statistics, surveys
- Controls, regulatory and compliance frameworks

# What could go wrong?

- Ransowmare
- Supply chain attacks
- People – social engineering, phishing
- Vulnerabilities
- …

# Ransomware

- Johnson Controls (2023)
  - Dark Angels ransomware gang ($51 mil. ransom, 27 TB of data stolen)
  - unauthorized access, data exfiltration, deployment of ransomware
  - shut down large portion of IT
  - cost of response and remediation: 27 mil. USD
- Colonial Pipeline (2021)
  - pipeline system for gasoline, diesel and jet fuel
  - DarkSide malware, billing infrastructure affected, 100 GB exfiltrated
  - pipeline shutdown as a prevention
  - ransom paid within hours (75 BTC $\sim$ 4.4 mil USD) – decryption tool too slow
  - panic buying, fuel shortages, state of emergency declared by POTUS
  - pipeline operations restored after six days
  - DarkSide: "*our goal is to make money, and not creating problems for society*"

# Supply chain attack: SolarWinds

- reported by FireEye in December 2020
- Solorigate, Sunburst, UNC2452
- SolarWinds Orion platform
  - infrastructure monitoring and management platform designed to simplify IT administration for on-premises, hybrid, and software as a service (SaaS) environments
  - Network Performance Monitor, NetFlow Traffic Analyzer, Network Configuration Manager, Log Analyzer, Server & Application Monitor, Server Configuration Monitor, and other components
- Malware in updates (released between March 2020 and June 2020)
  - *see timeline*
  - supply chain attack
  - build process compomised
  - allowed to deploy aditional malware on customers' networks
  - C&C domain seized in December 2020 and used as "killswitch"

# SolarWinds hack cont.

- Impacted customers:
  - 18.000 with trojanized version of Orion platform
  - major contractor for US Government
  - Pentagon, Department of Energy, Department of Homeland Security, National Institute of Health, Department of Treasury, Department of Commerce, etc.
  - Microsoft, CrowdStrike, Fidelis, FireEye, Palo Alto Networks, Qualys etc.

# Vulnerability: HTTP/2 Rapid Reset

- Cloudflare, Google, AWS (CVE-2023-44487)
  - first exploited and observed in August 2023
  - Cloudflare: peak DDoS – 201 million requests/s (botnet with only 20.000 machines)
  - Google: peak DDoS – 398 million requests/s
  - AWS: peak DDoS – 155 million requests/s
- root cause
  - HTTP/2 features: stream multiplexing and concurrency
  - abusing ability to reset (cancel) stream immediately
  - sending large number of requests that are immediateley reset
- fixed in various web server and reverse proxy implementations

# Vulnerability: Exchange Server

- 4 vulnerabilities fixed (out-of-band) in March 2021
  - exploited since January (at least)
  - CVE-2021-26855: unauthenticated attacker can send HTTP requests and authenticate as the Exchange Server (SSRF)
  - CVE-2021-26858, CVE-2021-27065: post-authentication arbitrary file write vulnerabilities
  - CVE-2021-26857: post-authentication RCE as SYSTEM
  - in the codebase of Exchange Server for more than 10 years
- initial attacks attributed to Hafnium group (by Microsoft)
- impact: persistent system access, access to data, ransomware
- PoC available/removed from Github
- CISA Emergency Directive 21-02

# Vulnerability: Log4Shell

- reported by Alibaba Cloud Security Team (CVE-2021-44228 and few other)
- publicly disclosed in December 2021
- unnoticed since 2013
- problems with Log4j library (*see picture*)
  - string substitution while logging
  - for example remote data from evil LDAP server, log4j deserializes Java class and executes it
- impact: RCE, easy to exploit
- almost everyone patching/fixing/mitigating
- CISA Emergency Directive 22-02

# Vulnerability: VMware

- some products patched in April 2022
  - CVE 2022-22954: remote code execution
  - CVE 2022-22960: escalate to root
  - reverse engineered and first exploitations in 48 hours
- two additional vulnerabilities in May 2022
  - CVE-2022-22972: obtain administrative access without authentication
  - CVE-2022-22973: escalate to root
- CISA Emergency Directive 22-03

# Security incidents and failures

- various causes (or their combination): human factor, criminal activities, technical vulnerabilities etc.
- impact: “nothing” happened, loss of reputation, cost of repair/replacement of data and systems, direct financial loss, bankruptcy etc.

Vulnerabilities (usually SW):

- reality is worse (unpublished vulnerabilities, weak passwords, misconfiguration, etc.)
- National Vulnerability Database (nvd.nist.gov)
- various other sources exist
  - more sources and vulnerabilities covered, faster publication, additional detail (e.g. how to fix), …
- Known Exploited Vulnerabilities Catalog
  - subset of NVD, managed by CISA
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# NVD

- operated by NIST
- vulnerabilities (software flaws) published:

| year | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|---|---|
| count | 16509 | 17305 | 18350 | 20155 | 25050 | 28829 |

- includes additional information
  - classification (categories, severity score etc.)
  - affected software
  - links to other sources

# NVD – the most prevalent categories in 2023

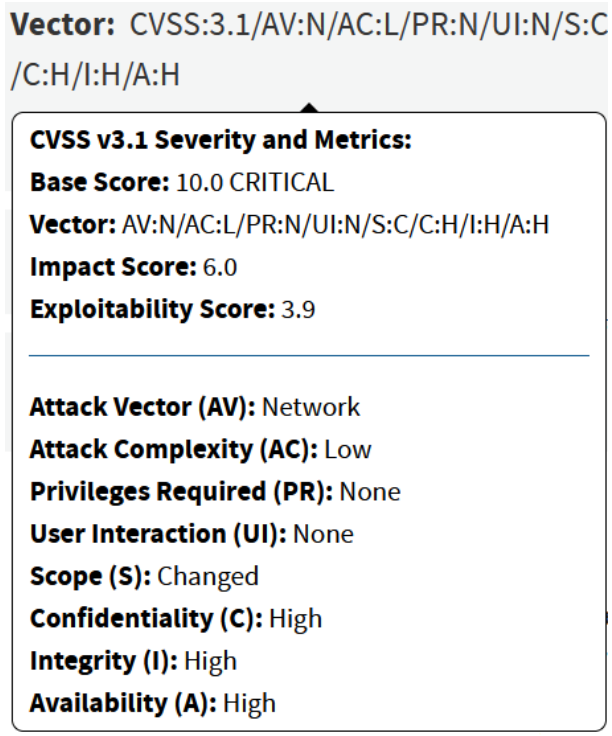
source: https://nvd.nist.gov/rest/public/visual/vulns/cwe/percentages

| % | CWE | Title |
|---|---|---|
| 39.67 | Miscellaneous | Miscellaneous |
| 14.56 | NVD-CWE-noinfo | Insufficient Information |
| 8.32 | CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| 6.15 | CWE-787 | Out-of-bounds Write |
| 3.39 | CWE-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| 2.33 | CWE-862 | Missing Authorization |
| 2.19 | CWE-125 | Out-of-bounds Read |
| 2.00 | CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 1.65 | CWE-352 | Cross-Site Request Forgery (CSRF) |
| 1.59 | CWE-120 | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |
| 1.54 | CWE-416 | Use After Free |
| 1.37 | CWE-77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| 1.34 | CWE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| 1.22 | CWE-434 | Unrestricted Upload of File with Dangerous Type |
| 0.95 | CWE-287 | Improper Authentication |
| 0.93 | CWE-20 | Improper Input Validation |
| 0.80 | CWE-863 | Incorrect Authorization |
| 0.72 | CWE-476 | NULL Pointer Dereference |
| 0.67 | CWE-400 | Uncontrolled Resource Consumption |
| 0.64 | CWE-94 | Improper Control of Generation of Code ('Code Injection') |
| 0.61 | CWE-668 | Exposure of Resource to Wrong Sphere |
| 0.58 | CWE-190 | Integer Overflow or Wraparound |
| 0.54 | CWE-269 | Improper Privilege Management |
| 0.50 | CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |
| 0.50 | CWE-798 | Use of Hard-coded Credentials |
| … | … | … |

# Examples … (1)

CVE-2021-44228 (CWE-502 Deserialization of Untrusted Data)

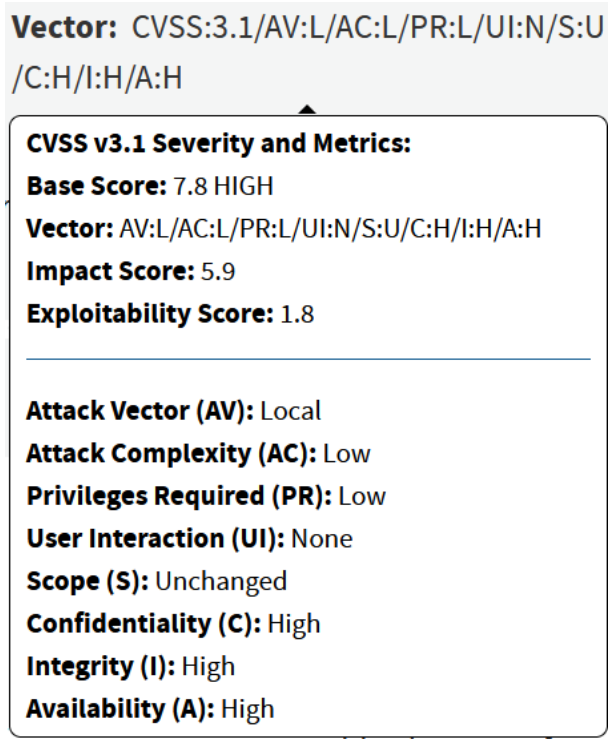
*Apache Log4j2 2.0-beta9 through 2.15.0 (…) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. ….*



# Examples … (2)

CVE-2022-22960 (CWE-269 Improper Privilege Management):

*VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts. A malicious actor with local access can escalate privileges to 'root'.*

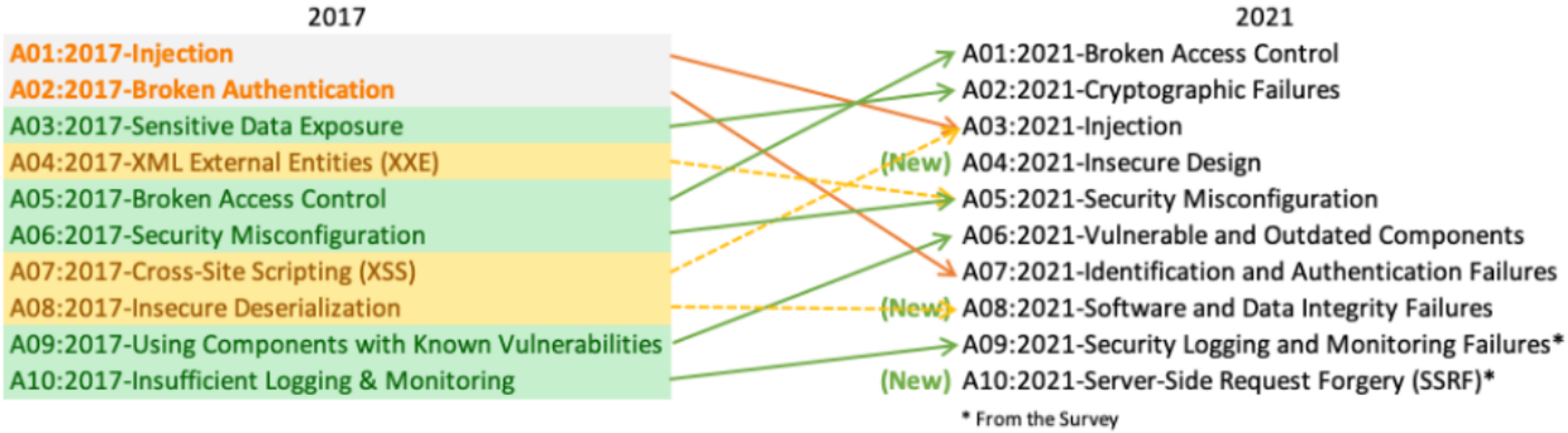


# Other classifications (MITRE)

- Common Vulnerabilities and Exposures (cve.mitre.org)
  - vulnerabilities ~ NVD (NVD contains more information)
- Common Weaknesses Enumeration (cwe.mitre.org)
  - buffer overflows, XSS, CSRF, code injection, etc.
- Common Attack Pattern Enumeration and Classification (capec.mitre.org)
  - attack hierarchies, description, prerequisites, mitigation, CWE link, etc.
- ATT&CK – Adversary tactics and techniques (attack.mitre.org)
  - knowledge base, ATT&CK for Enterprise, ATT&CK for Mobile
- Common Platform Enumeration (MITRE → NIST, nvd.nist.gov/products/cpe)
  - dictionary for IT systems, software, and packages
  - can describe version, release, platform etc.

# OWASP

- Open Web Application Security Project (OWASP, www.owasp.org)
- primarily for web applications – vulnerabilities, attacks, risks
- OWASP Top 10 (most critical web application security risks, 2021)
- Web Security Testing Guide (v4.2, 2020)
- Application Security Verification Standard (v4.0.3, 2021)
- Mobile Application Security Testing Guide (v1.7.0, 2023)
- Mobile Application Security Verification Standard (v2.1.0, 2024)

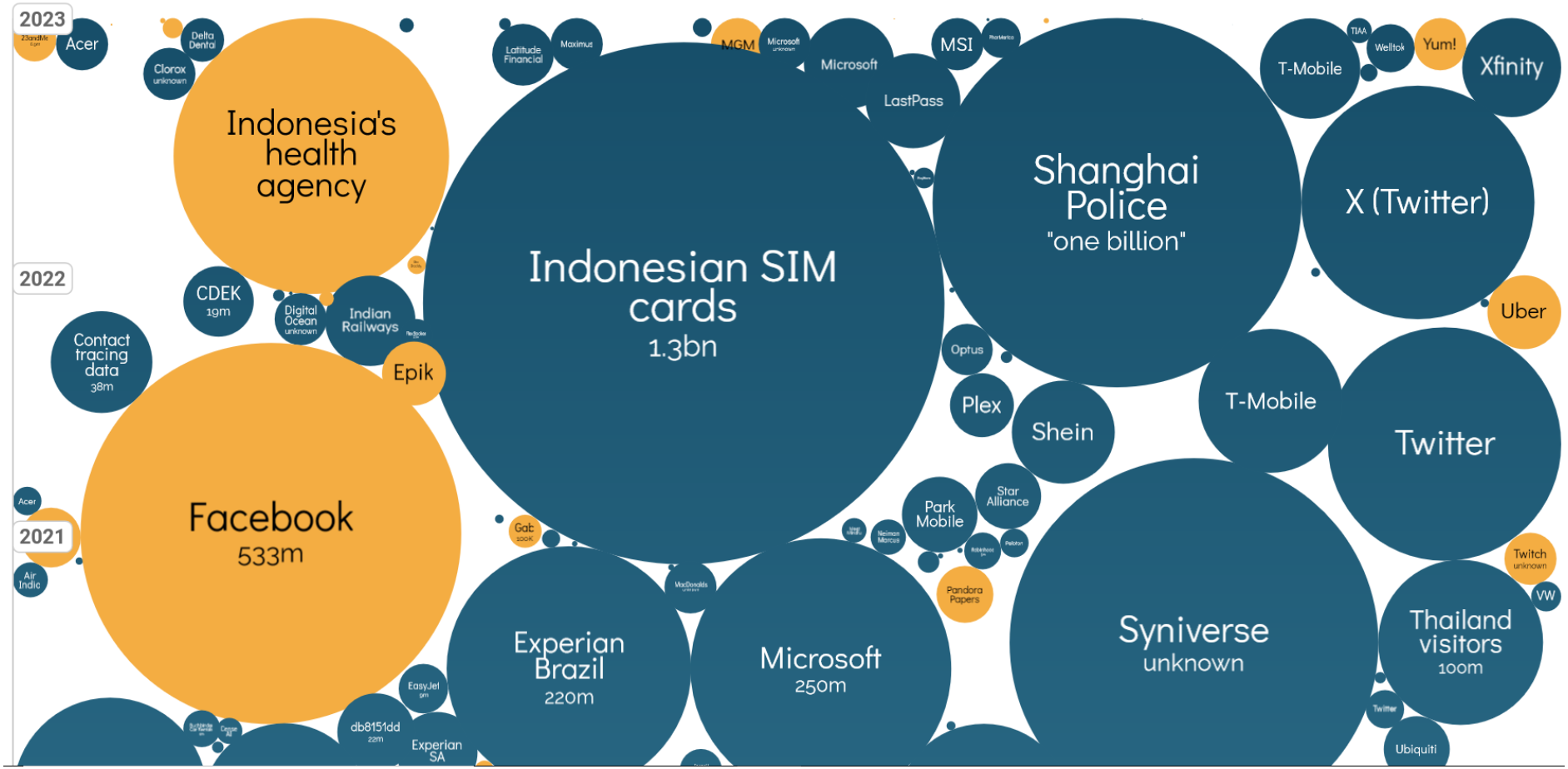



source: OWASP, owasp.org/www-project-top-ten

# Real world

- not everything is published or shared
- sometimes you just don't know yet
- sometimes you are just lucky

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



# EY Global Information Security Survey 2021

- more than 1.000 respondents
- senior cybersecurity professionals (e.g. CISO)
- *extremely confident in their organization's cybersecurity risk*
  - 9% in 2021 (20% in 2020)
- the problems:
  - insufficient budget – realigned cybersecurity, cost-reduction
  - complex new regulations – drain of time and resources
  - deteriorating relationship with business leaders

# Verizon: 2023 Data Breach Investigations Report

- summary of 1 year (incidents Nov 21 – Oct 22)
- global coverage, detailed, 89 pages
- Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach: An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.
- datasets contributed by various security vendors
- analysis includes ~ 16 312 security incidents, and ~ 5 199 confirmed data breaches
- the report provides details for 10 industries

# Verizon – 2023 DBIR – patterns

- patterns in incidents (see Fig. 25):

  DoS > System intrusion > Lost and stolen assets >
  Social Engineering > Basic web application attacks > ...
- patterns in breaches (see Fig. 26):

  System intrusion > Basic web application attacks >
  Social Engineering > Miscellaneous errors > Privilege misuse > ...

# Verizon – 2023 DBIR – some observations

- breaches – threat actor motivation – 95% financial
- ransomware (24% of breaches, 16% of incidents)
- breaches – action:
  exploit vulnerabilities (5%) vs. use of stolen credentials (45%)
- rising social engineering (17% breaches, 10% incidents)
- organizations' median time to patch critical vulnerabilities: 49 days

# What to do – Controls, regulatory and compliance frameworks

# What to do – regulatory and compliance frameworks

- NIST SP 800-53 (Rev. 5) Security and Privacy Controls for Information Systems and Organizations (2020)
  - supplemental material – mappings, control catalog, templates
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls
  - best practice recommendations on information security controls
  - open to interpretation (good and bad)
- NIST Cybersecurity Framework (Version 2.0, 2024)
  - set of desired cybersecurity activities and outcomes using (easy to understand) common language
  - version 2.0 should be released at the end of February 2024

# NIST Cybersecurity Framework – (2.0 Draft)

| Function | Category | Category Identifier |
|---|---|---|
| **Govern (GV)** | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policies, Processes, and Procedures | GV.PO |
| | Oversight | GV.OV |
| **Identify (ID)** | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Improvement | ID.IM |
| **Protect (PR)** | Identity Management, Authentication, and Access Control | PR.AA |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Platform Security | PR.PS |
| | Technology Infrastructure Resilience | PR.IR |
| **Detect (DE)** | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| **Respond (RS)** | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| **Recover (RC)** | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |

# What to do – regulatory and compliance frameworks (2)

- Australian Government Information Security Manual (2023)
- ISACA: COBIT 5 Framework
- Payment Card Industry – Data Security Standard version 4.0 (PCI DSS, 2022)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ...
- Zákon č. 95/2019 Z. z. o ITVS, Vyhláška č. 179/2020 Z. z. (spôsob kategorizácie a obsah bezpečnostných opatrení)
- CIS Critical Security Controls (v8, 2021)
  - 18 controls, 153 safeguards
  - implementation groups IG1 (essential cyber hygiene), IG2 and IG3

# CIS Controls v8 – controls

https://www.cisecurity.org/controls/

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser and Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense

# CIS Controls v8 – controls (2)

14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

# UK: Cyber Essentials Scheme

https://www.ncsc.gov.uk/cyberessentials

- Cyber Essentials: Requirements for IT infrastructure (v3.1, 2023)
  - just basic controls, 16 pages
  - clear guidance what is in scope and what to do
- Cyber Essentials (self-assessment, verification)
- Cyber Essentials Plus (hands-on technical verification)
- Technical control themes:
  1. Firewalls
  2. Secure configuration
  3. Security update management
  4. User access control
  5. Malware protection