Praxisbeispiel CyberSecurity in der Revision

CIS Framework und Logdaten Analysen
English subtitle: CIS framework and logs-based analytics

Babatope Aloba, Internal Audit

Vienna, April 2024

Empowering
Communities to Progress.

Bank Austria
Member of UniCredit

Agenda

1 Speaker profile, Company profile

2 Audit Background and Audit approach

3 CIS framework => Audit work program (2 slides)

4 Sampling vs Data analytics

5 Selected Audit Tests and Results

6 Questions

Speaker profile, Company profile (1/3)

Speaker Bio

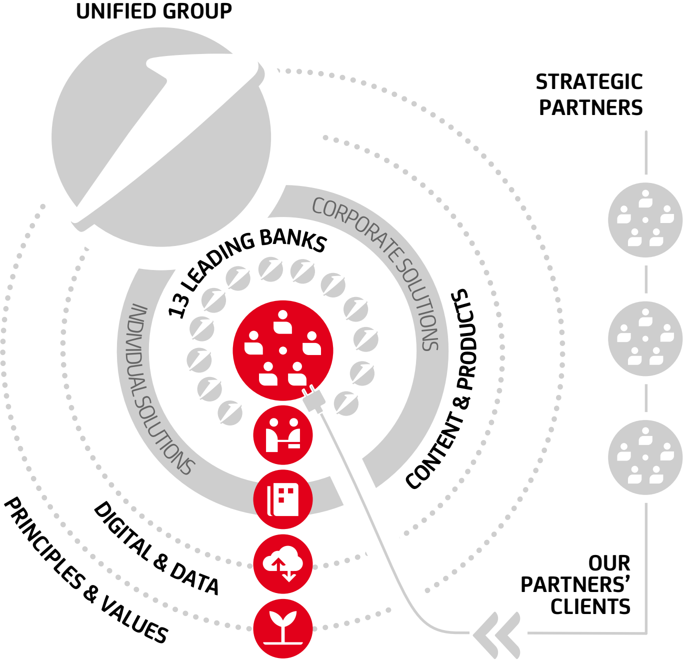
Name:	Babatope Aloba, CISA
Education:	Business Informatics, Vienna University of Technology
Present/past Roles:	ICT & Cybersecurity Auditor, IT-Auditor, Internal Auditor, SOX-Auditor, Software Engineer/Database developer
Hobbies:	Virtual hobbies: Information security: Firewalls, anti-spam techniques, AI Real world hobbies: travelling & sightseeing. Last travel destination: Japan (March 2024)

Speaker profile, Company profile (2/3)

UniCredit Group – who we are

At a glance: a pan-European Group[1]

A pan-European Commercial Bank connecting with clients in a unified way across Europe



UNIFIED GROUP

STRATEGIC PARTNERS

13 LEADING BANKS

CORPORATE SOLUTIONS

INDIVIDUAL SOLUTIONS

CONTENT & PRODUCTS

DIGITAL & DATA

PRINCIPLES & VALUES

OUR PARTNERS' CLIENTS

13 Banks

81k people

4 Coverage regions

1 leaner Corporate Centre embedding Digital & data

2 product factories serving all regions

A pan-European Commercial Bank connecting with clients in a unified way across Europe

[1] Data as of 31.12.2022

https://www.unicreditgroup.eu/content/dam/unicreditgroup-eu/documents/en/banking-group/at-a-glance/UniCreditGroupCompanyProfile.pdf

Speaker profile, Company profile (2/3)

UniCredit Group – our strategy

UniCredit Unlocked: our Digital revolution

From USING digital to LIVING digital

Being the Bank for Europe's future means becoming an **integrated, fast and efficient digital bank**, using state of the art, cloud-based infrastructure. We will use **Data** to empower our decision making, to continuously adapt to a shifting market, and to offer a best-in-class customer experience.

We will leverage on **four global pillars** in our organisation: reclaim core competencies, a new way of working, reshape our architecture and improve resilience and build digital experience.

This will drive our overarching Group digital development and the countries will deliver the last mile products, tailored to the **local needs**.

We want to gain the right competences and technology to create a **seamless digital offering** that will serve our clients anywhere & anytime, exceeding their expectations.

Audit Background and Audit approach

Task:

...create a standard work program focused on cybersecurity, based on our risk profile (and our subsidiaries) and flexibly scalable under the following constraints:

- Adjustable to the different sizes and risk profiles of our subsidiaries,
- Adjustable to reflect the unique risk profile of each legal entity
- Adjustable to audit the most relevant processes and systems being used at each legal entity
- Support a data driven audit as much as possible

Solution:

... use one or multiple standard frameworks and emphasize audit tests that can be enhanced through the use of data analytics

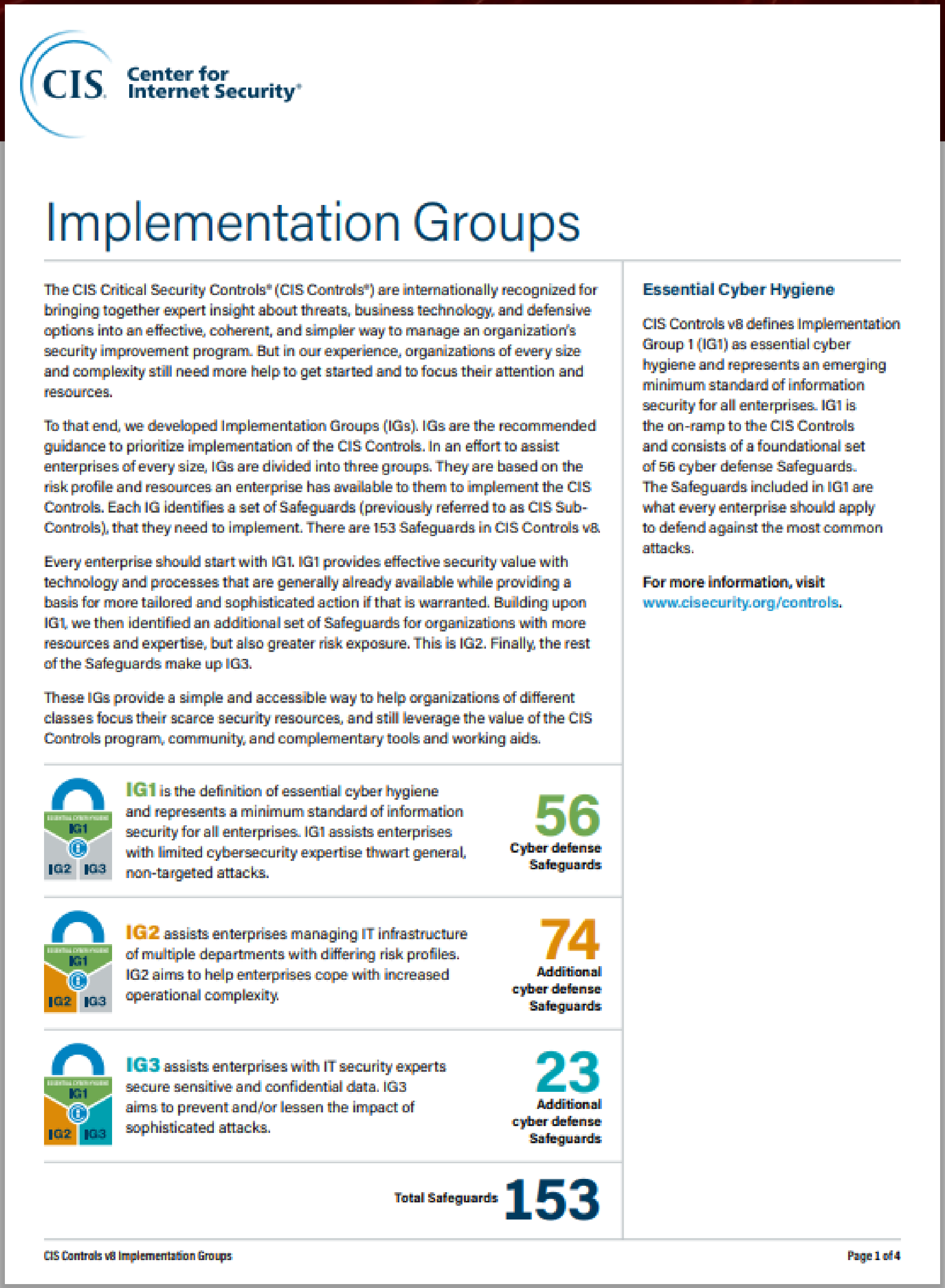
CIS framework => Audit work program (1/2)

CIS-Framework (v8) at a glance

- CIS Critical Security Controls® (CIS Controls®) are/were …
- … initially developed by NIST,
- … constantly evolving, development led by CIS – Center for Internet Security,
- … describe a set of activities (18 controls which include a total of 153 safeguards) to ensure that:

  CIS Security Best Practices (which include the CIS Controls and CIS Benchmarks) are more than a checklist of "good things to do," or "things that could help"; instead, they are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements,

- … structured to allow customization to different organization sizes, complexities and risk profiles using so-called **"Implementation Groups"**



CIS Center for Internet Security®

Implementation Groups

The CIS Critical Security Controls® (CIS Controls®) are internationally recognized for bringing together expert insight about threats, business technology, and defensive options into an effective, coherent, and simpler way to manage an organization's security improvement program. But in our experience, organizations of every size and complexity still need more help to get started and to focus their attention and resources.

To that end, we developed Implementation Groups (IGs). IGs are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There are 153 Safeguards in CIS Controls v8.

Every enterprise should start with IG1. IG1 provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action if that is warranted. Building upon IG1, we then identified an additional set of Safeguards for organizations with more resources and expertise, but also greater risk exposure. This is IG2. Finally, the rest of the Safeguards make up IG3.

These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

Essential Cyber Hygiene

CIS Controls v8 defines Implementation Group 1 (IG1) as essential cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

For more information, visit www.cisecurity.org/controls.

CIS Controls v8 Implementation Groups

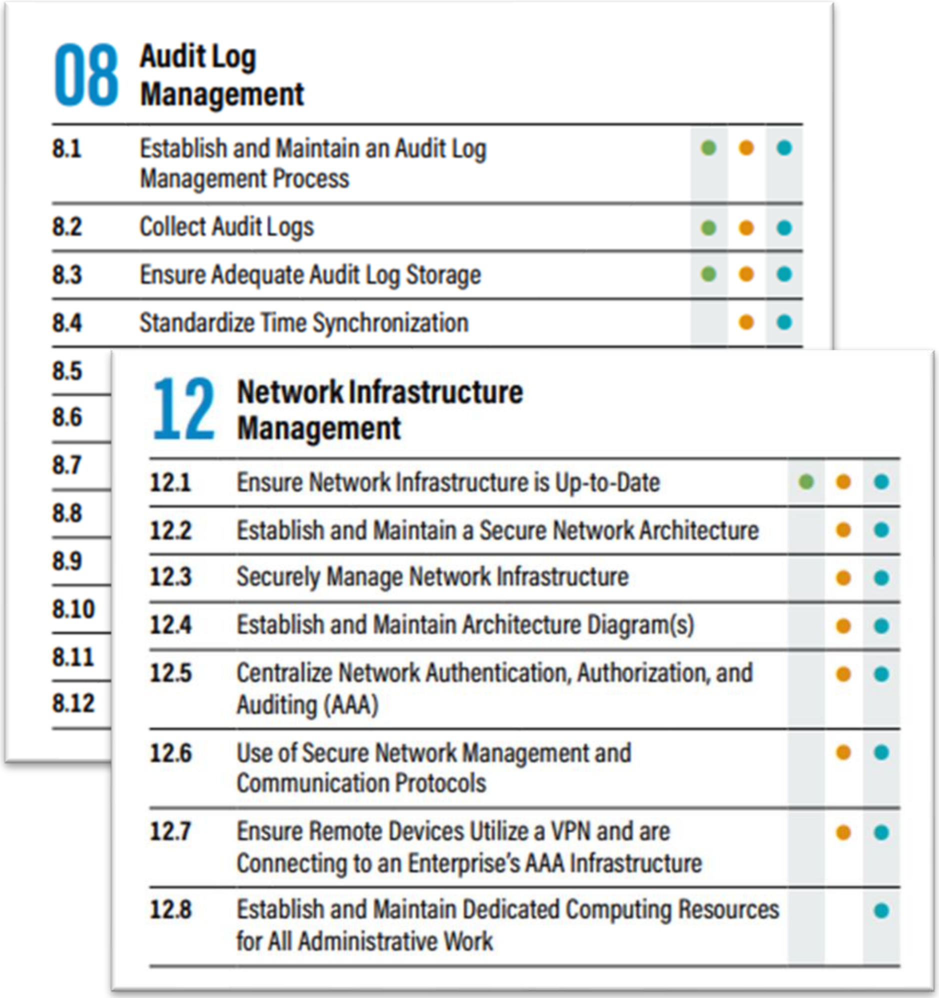
Page 1 of 4

CIS Controls® - http://www.cisecurity.org/controls/

CIS framework => Audit work program (2/2)

UCBA tailored work program for IG1 (subset-excerpt)

- CIS framework‘s IG1 consists of 18 a total of 56 safequards: this was still too much => focus on fewer safeguards, but specifically including CIS08 and CIS12

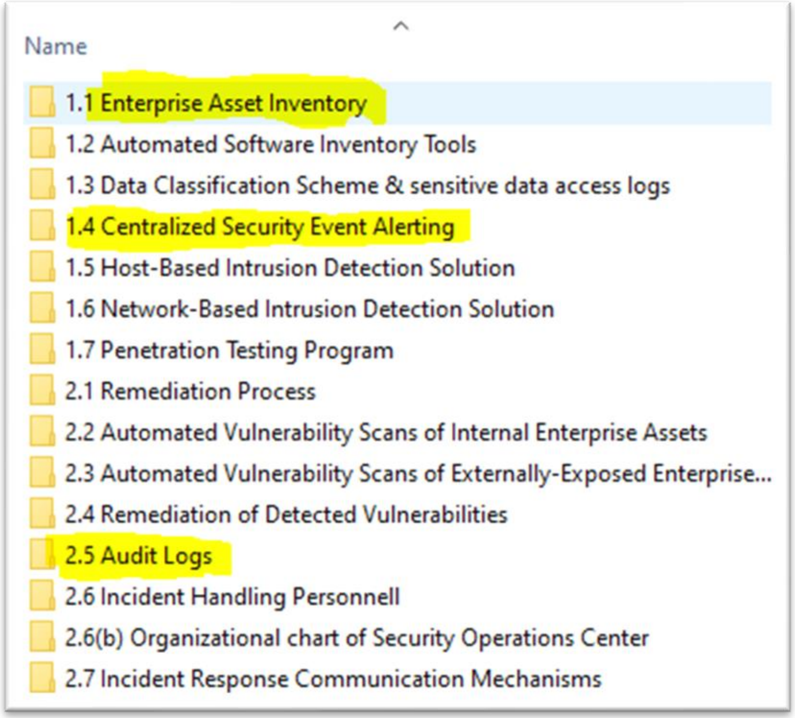


08 Audit Log Management

8.1	Establish and Maintain an Audit Log Management Process	●	●	●
8.2	Collect Audit Logs	●	●	●
8.3	Ensure Adequate Audit Log Storage	●	●	●
8.4	Standardize Time Synchronization		●	●
8.5				
8.6				
8.7				
8.8				
8.9				
8.10				
8.11				
8.12				

12 Network Infrastructure Management

12.1	Ensure Network Infrastructure is Up-to-Date	●	●	●
12.2	Establish and Maintain a Secure Network Architecture		●	●
12.3	Securely Manage Network Infrastructure		●	●
12.4	Establish and Maintain Architecture Diagram(s)		●	●
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		●	●
12.6	Use of Secure Network Management and Communication Protocols		●	●
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		●	●
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			●



Name

- 1.1 Enterprise Asset Inventory
- 1.2 Automated Software Inventory Tools
- 1.3 Data Classification Scheme & sensitive data access logs
- 1.4 Centralized Security Event Alerting
- 1.5 Host-Based Intrusion Detection Solution
- 1.6 Network-Based Intrusion Detection Solution
- 1.7 Penetration Testing Program
- 2.1 Remediation Process
- 2.2 Automated Vulnerability Scans of Internal Enterprise Assets
- 2.3 Automated Vulnerability Scans of Externally-Exposed Enterprise...
- 2.4 Remediation of Detected Vulnerabilities
- 2.5 Audit Logs
- 2.6 Incident Handling Personnell
- 2.6(b) Organizational chart of Security Operations Center
- 2.7 Incident Response Communication Mechanisms

IG1: 56 safeguards

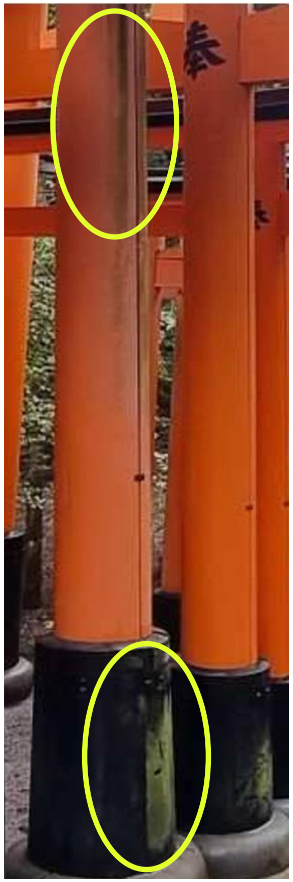
Tailored WP: 15 safeguards

Sampling vs Data Analytics (1/2)

Sampling dilemma

© Babatope Aloba, 2024

Fushimi Inari Taisha in Kyoto, Japan



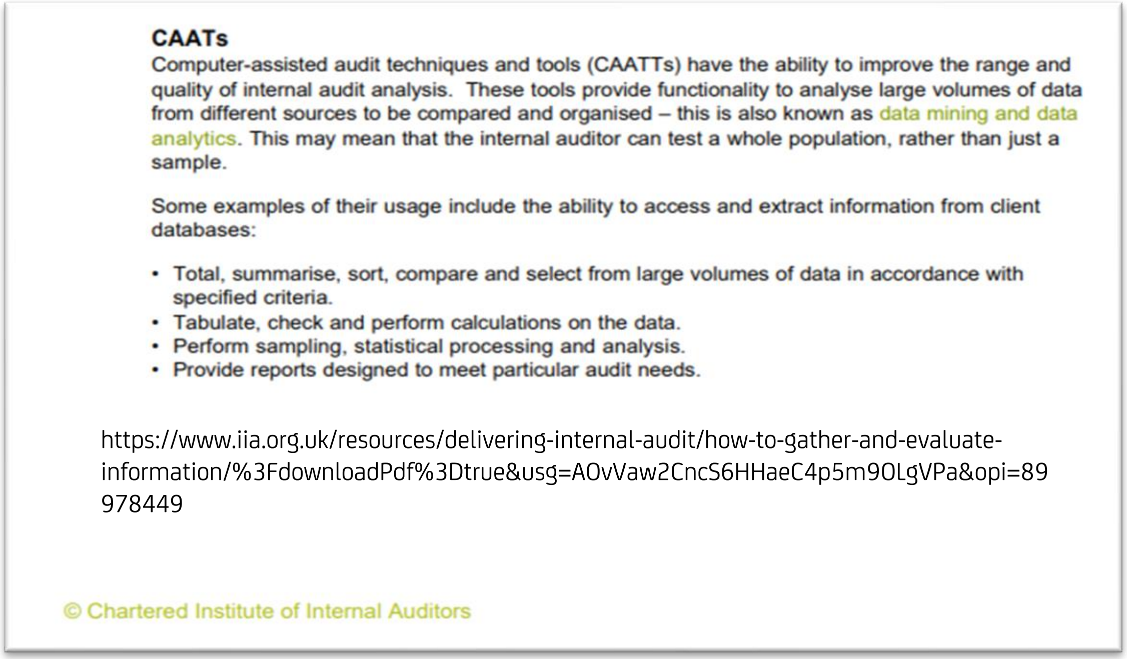
© Babatope Aloba, 2024

Sampling vs Data Analytics (2/2)

Sampling vs Population testing

Performing transaction tests on entire populations rather than just testing samples lets auditors consider broader sets of audit relevant data and thus produce higher quality audit evidence.

Source: https://cfrr.worldbank.org/sites/default/files/2019-11/SMPs_spreads_digital.pdf



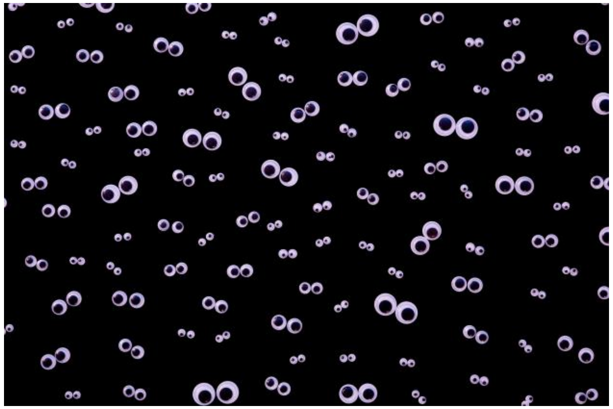
CAATs

Computer-assisted audit techniques and tools (CAATTs) have the ability to improve the range and quality of internal audit analysis. These tools provide functionality to analyse large volumes of data from different sources to be compared and organised – this is also known as data mining and data analytics. This may mean that the internal auditor can test a whole population, rather than just a sample.

Some examples of their usage include the ability to access and extract information from client databases:

- Total, summarise, sort, compare and select from large volumes of data in accordance with specified criteria.
- Tabulate, check and perform calculations on the data.
- Perform sampling, statistical processing and analysis.
- Provide reports designed to meet particular audit needs.

https://www.iia.org.uk/resources/delivering-internal-audit/how-to-gather-and-evaluate-information/%3FdownloadPdf%3Dtrue&usg=AOvVaw2CncS6HHaeC4p5m9OLgVPa&opi=89978449



Selected Audit Tests & Results

WP Test - Audit logs for Subsidiary XYZ

Document/evidence request to be provided by Auditees:

- CMDB extract of all Configuration Items (CIs)
- SIEM extract for selected time frame

Tests performed:

- Inventory completeness check part 1: do all devices have logs enabled? (review configuration settings)
- Inventory completeness check part 2: are logs for all devices in the CMDB in the SIEM? => Big-Data analytics
- Inventory completeness check part 3: are all devices logging to the SIEM registered in the CMDB? => Big-Data analytics

Findings:

Criteria:

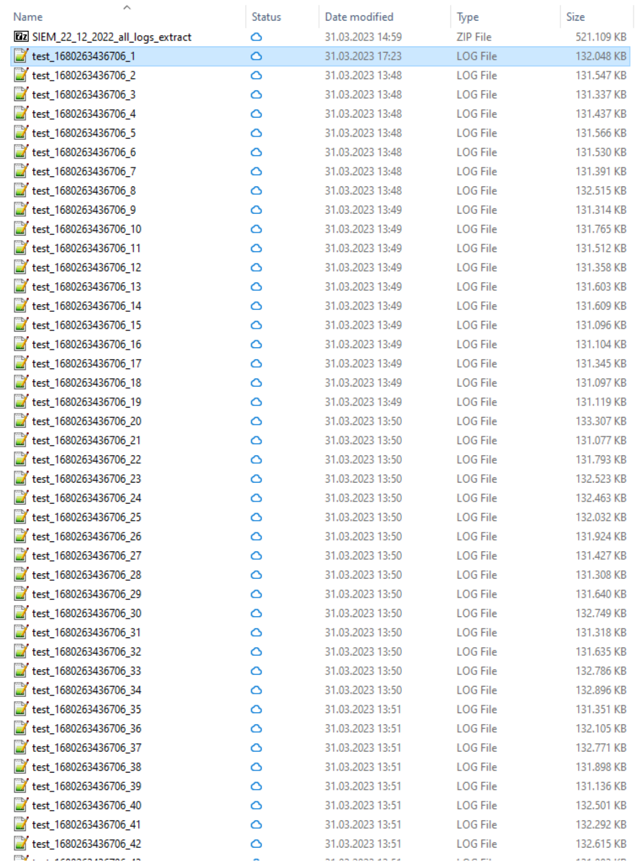
CIS Control 8.2 Collect Audit Logs:
Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.

Condition:

Logging was not activated for all CIs - systems, devices and containers.

Root cause(s):

- Misconfiguration of VMWare logging levels (0-5)
- Incomplete inventory of containers and container-based services
- Misconfiguration of firewall settings which blocked ports required for logging



Name	Status	Date modified	Type	Size
SIEM_22_12_2022_all_logs_extract	☁	31.03.2023 14:59	ZIP File	521.109 KB
test_1680263436706_1	☁	31.03.2023 17:23	LOG File	132.048 KB
test_1680263436706_2	☁	31.03.2023 13:48	LOG File	131.547 KB
test_1680263436706_3	☁	31.03.2023 13:48	LOG File	131.337 KB
test_1680263436706_4	☁	31.03.2023 13:48	LOG File	131.437 KB
test_1680263436706_5	☁	31.03.2023 13:48	LOG File	131.566 KB
test_1680263436706_6	☁	31.03.2023 13:48	LOG File	131.530 KB
test_1680263436706_7	☁	31.03.2023 13:48	LOG File	131.391 KB
test_1680263436706_8	☁	31.03.2023 13:48	LOG File	132.515 KB
test_1680263436706_9	☁	31.03.2023 13:49	LOG File	131.314 KB
test_1680263436706_10	☁	31.03.2023 13:49	LOG File	131.765 KB
test_1680263436706_11	☁	31.03.2023 13:49	LOG File	131.512 KB
test_1680263436706_12	☁	31.03.2023 13:49	LOG File	131.358 KB
test_1680263436706_13	☁	31.03.2023 13:49	LOG File	131.603 KB
test_1680263436706_14	☁	31.03.2023 13:49	LOG File	131.609 KB
test_1680263436706_15	☁	31.03.2023 13:49	LOG File	131.096 KB
test_1680263436706_16	☁	31.03.2023 13:49	LOG File	131.104 KB
test_1680263436706_17	☁	31.03.2023 13:49	LOG File	131.345 KB
test_1680263436706_18	☁	31.03.2023 13:49	LOG File	131.097 KB
test_1680263436706_19	☁	31.03.2023 13:49	LOG File	131.119 KB
test_1680263436706_20	☁	31.03.2023 13:50	LOG File	133.307 KB
test_1680263436706_21	☁	31.03.2023 13:50	LOG File	131.077 KB
test_1680263436706_22	☁	31.03.2023 13:50	LOG File	131.793 KB
test_1680263436706_23	☁	31.03.2023 13:50	LOG File	132.523 KB
test_1680263436706_24	☁	31.03.2023 13:50	LOG File	132.463 KB
test_1680263436706_25	☁	31.03.2023 13:50	LOG File	132.032 KB
test_1680263436706_26	☁	31.03.2023 13:50	LOG File	131.924 KB
test_1680263436706_27	☁	31.03.2023 13:50	LOG File	131.427 KB
test_1680263436706_28	☁	31.03.2023 13:50	LOG File	131.308 KB
test_1680263436706_29	☁	31.03.2023 13:50	LOG File	131.640 KB
test_1680263436706_30	☁	31.03.2023 13:50	LOG File	132.749 KB
test_1680263436706_31	☁	31.03.2023 13:50	LOG File	131.318 KB
test_1680263436706_32	☁	31.03.2023 13:50	LOG File	131.635 KB
test_1680263436706_33	☁	31.03.2023 13:50	LOG File	132.786 KB
test_1680263436706_34	☁	31.03.2023 13:50	LOG File	132.896 KB
test_1680263436706_35	☁	31.03.2023 13:51	LOG File	131.351 KB
test_1680263436706_36	☁	31.03.2023 13:51	LOG File	132.105 KB
test_1680263436706_37	☁	31.03.2023 13:51	LOG File	132.771 KB
test_1680263436706_38	☁	31.03.2023 13:51	LOG File	131.898 KB
test_1680263436706_39	☁	31.03.2023 13:51	LOG File	131.136 KB
test_1680263436706_40	☁	31.03.2023 13:51	LOG File	132.501 KB
test_1680263436706_41	☁	31.03.2023 13:51	LOG File	132.292 KB
test_1680263436706_42	☁	31.03.2023 13:51	LOG File	132.615 KB

SIEM extract for 24h:
500 Mb zipped logged files
12 Gb unzipped text files

Selected Audit Tests & Results

Summary – pros & cons

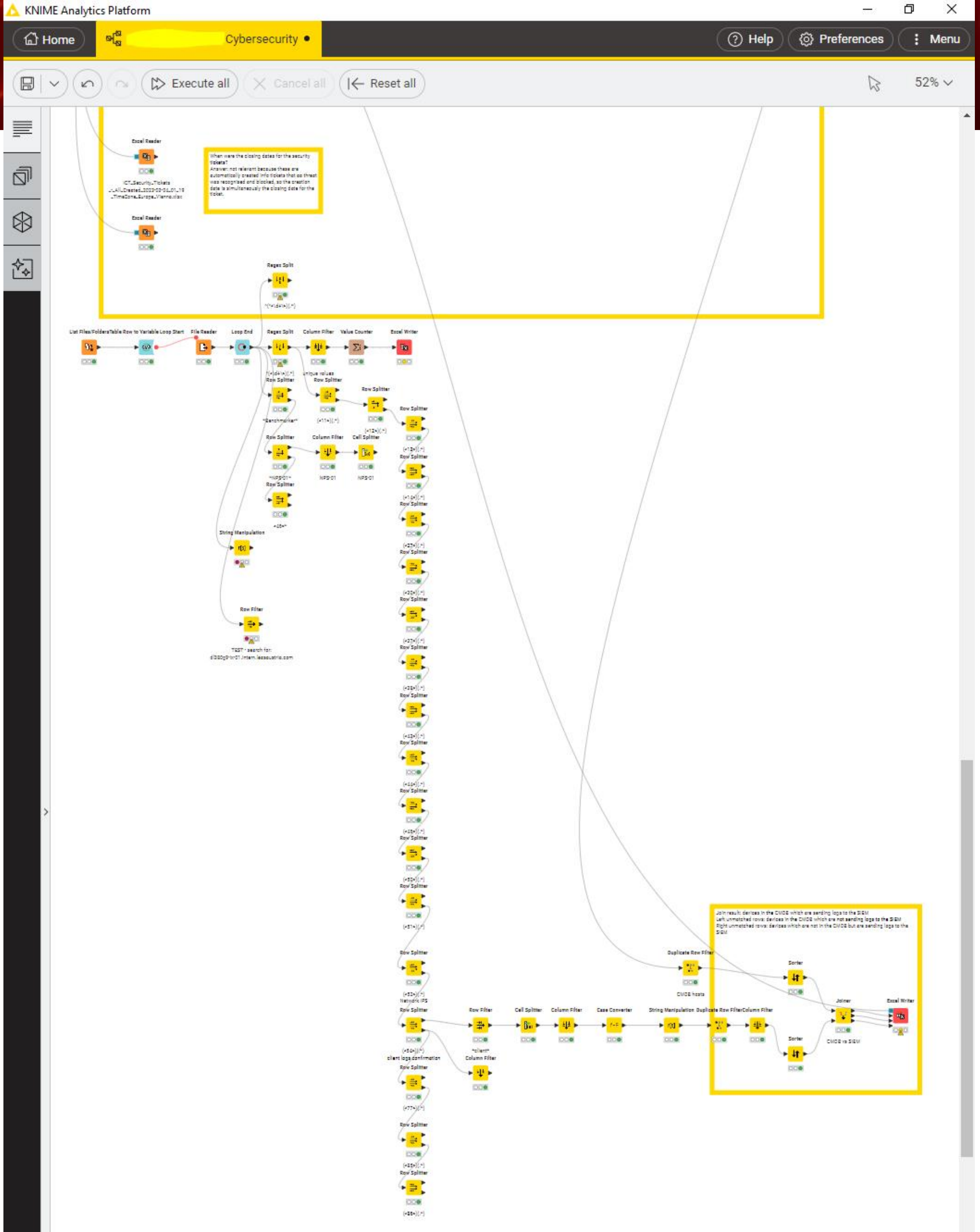
SUMMARY & CONCLUSIONS

Wins:

1. In depth analysis of full population was previously not possible. For example, the findings regarding completeness of logs would not have been possible.
2. Potential for advanced analytics identified – use of machine learning to establish a baseline pattern to enable detection of anomalies

Challenges:

1. Large dataset - each run of the analytics workflow took 15m to complete – resource intensive during development
2. SIEM structure was not normalized: different log formats coming from different systems, applications and services.



When were the closing dates for the security tickets?
Answer: not relevant because these are automatically created info tickets that as threat was recognised and blocked, so the creation date is simultaneously the closing date for the ticket.

Join result: devices in the CMDB which are sending logs to the SIEM
Left unmatched rows: devices in the CMDB which are not sending logs to the SIEM
Right unmatched rows: devices which are not in the CMDB but are sending logs to the SIEM

Questions?

Thank You!

This Photo by Unknown Author is licensed under CC BY

Thank You!

Danke schön!

どうもありがとうございます！

Dōmo arigatō gozaimasu!