Security at sciCOREmed

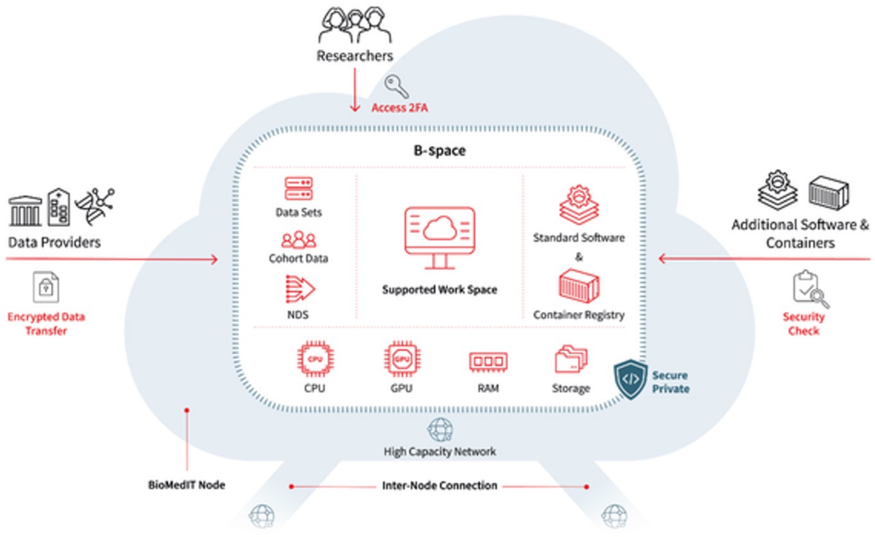
In collaboration with BioMedIT

hpc-ch forum on HPC Security / sciCORE, University of Basel / May 4th, 2023

sciCOREmed Introduction

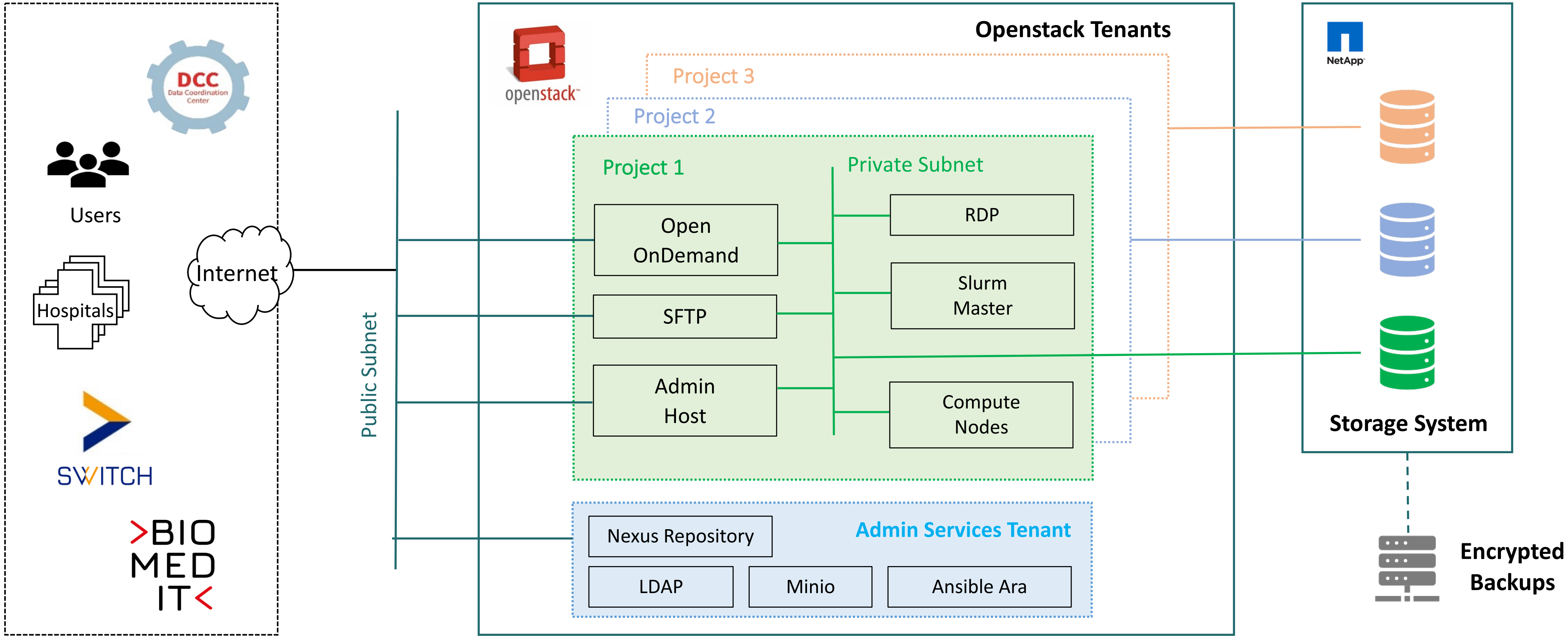
sciCOREmed provides a secure platform to perform research with sensitive personal data

- Operated by sciCORE
- One of the three nodes of BioMedIT network
- Built on OpenStack cloud
- Security by design



https://scicore.unibas.ch/projects/scicoremed/

sciCOREmed Architecture



Fog of More

Fog of More

Fog of War

"NEBEL DES KRIEGES"

Fog of More

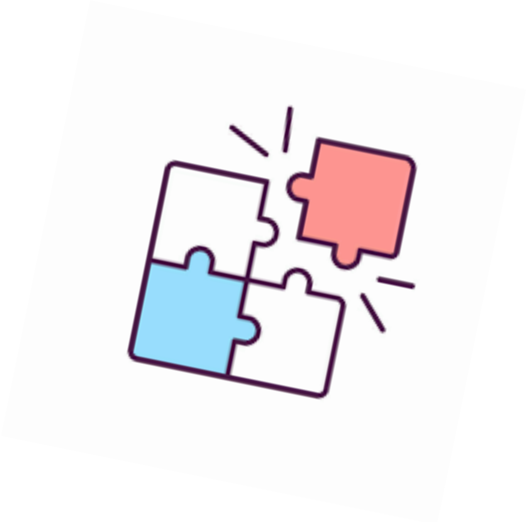
Cyber Defense
Security frameworks
Security tools and technologies
Vulnerability and exploit databases

IT Security Requirements
Risk management procedures
Compliance requirements
Regulatory mandates

Cyber Threat
Threat hunting
Threat Intelligence and sharing
Information feeds

Other Resources
Guidance and best practices
Benchmarks and checklists
Trainings and certifications

What to prioritize?



CIS Critical Security Controls

NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

"The SANS Top 20" (the SANS Institute)

The Critical Security Controls (CCS/CIS)

The CIS Controls™

Offense informs defense

Prioritization

Measurements and Metrics

Continuous diagnostics and mitigation

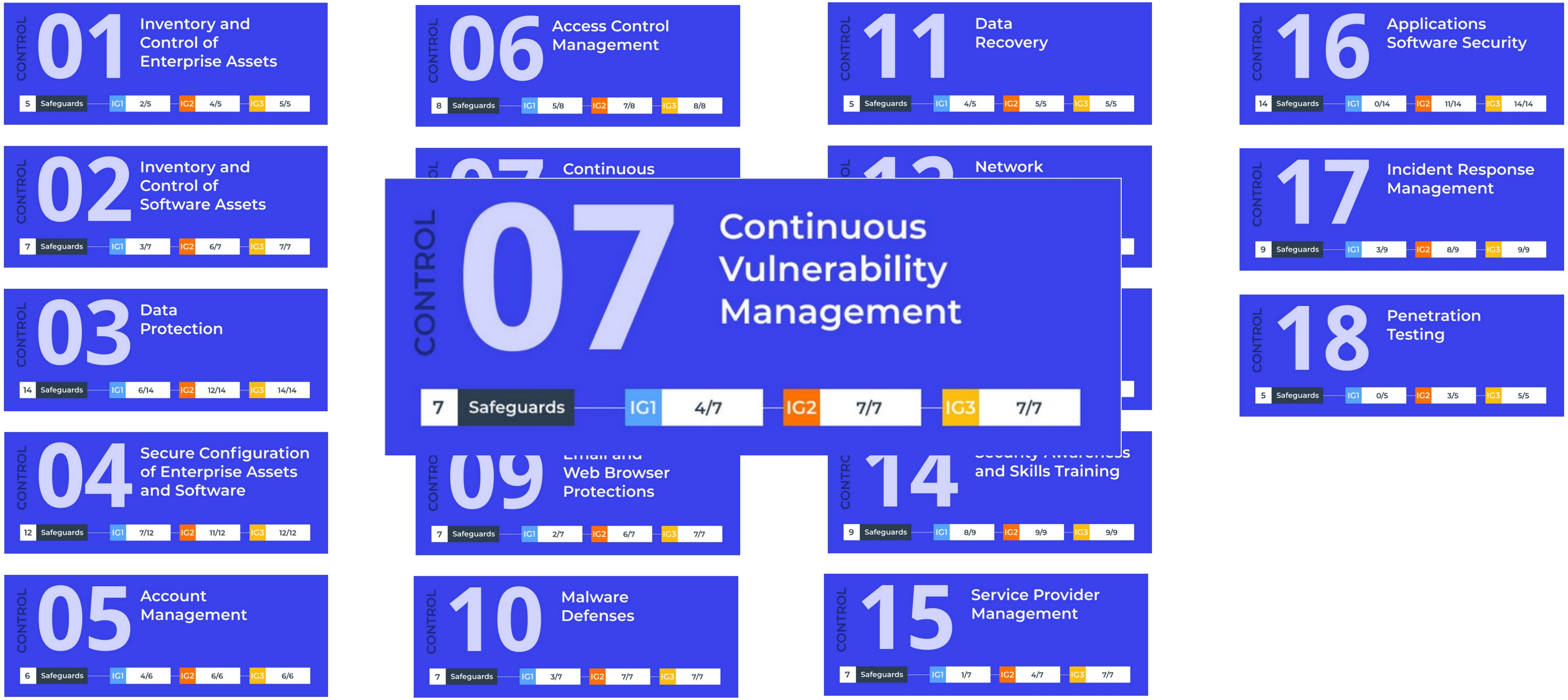
Automation

CIS Controls

CIS. Center for Internet Security®

https://www.cisecurity.org/insights/blog/how-prioritized-security-controls-break-through-the-fog-of-more

CIS Controls v8



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7

CONTROL 03 Data Protection
14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12

CONTROL 05 Account Management
6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8

Continuous

CONTROL 07 Continuous Vulnerability Management
7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7

CONTROL 09 Email and Web Browser Protections
7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5

Network

CONTROL 14 Security Awareness and Skills Training
9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9

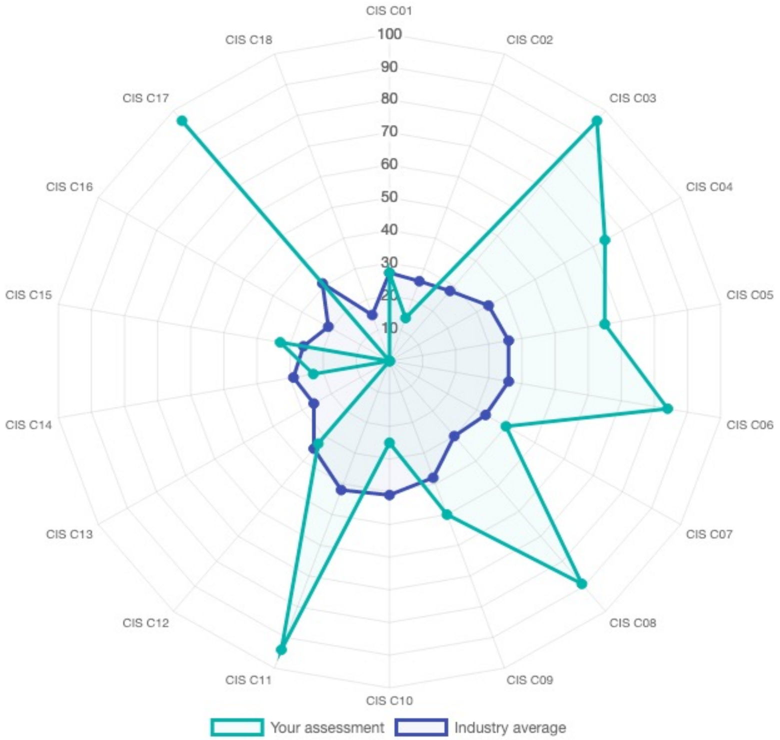
CONTROL 15 Service Provider Management
7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9

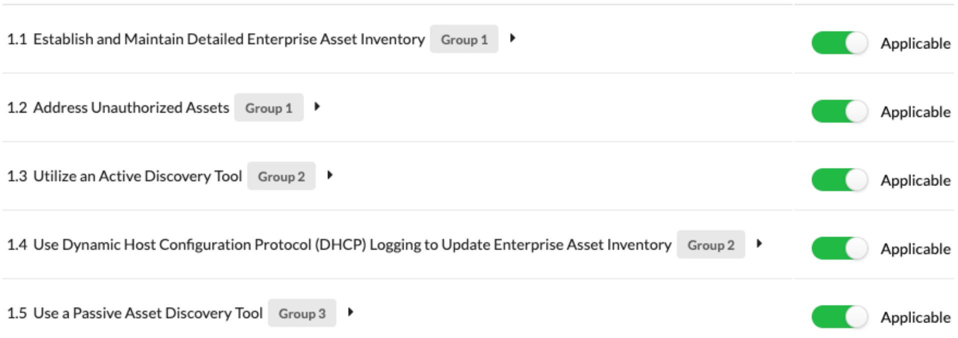
CONTROL 18 Penetration Testing
5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

CIS CSAT



[Not an assessment of sciCOREmed]

Inventory and Control of Enterprise Assets



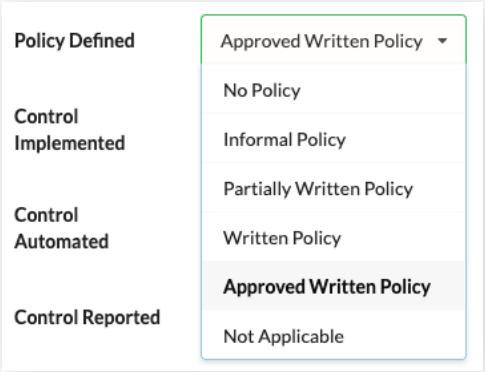
1.1 Establish and Maintain Detailed Enterprise Asset Inventory Group 1 ▸ Applicable

1.2 Address Unauthorized Assets Group 1 ▸ Applicable

1.3 Utilize an Active Discovery Tool Group 2 ▸ Applicable

1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory Group 2 ▸ Applicable

1.5 Use a Passive Asset Discovery Tool Group 3 ▸ Applicable



Policy Defined: Approved Written Policy ▾

- No Policy
- Informal Policy
- Partially Written Policy
- Written Policy
- **Approved Written Policy**
- Not Applicable

Control Implemented

Control Automated

Control Reported

CIS Implementation

How do we implement CIS controls?

BioMedIT Security WG

Mandate of the security working group is to address IT security and privacy issues specifically relevant in the context of the BioMedIT Project.

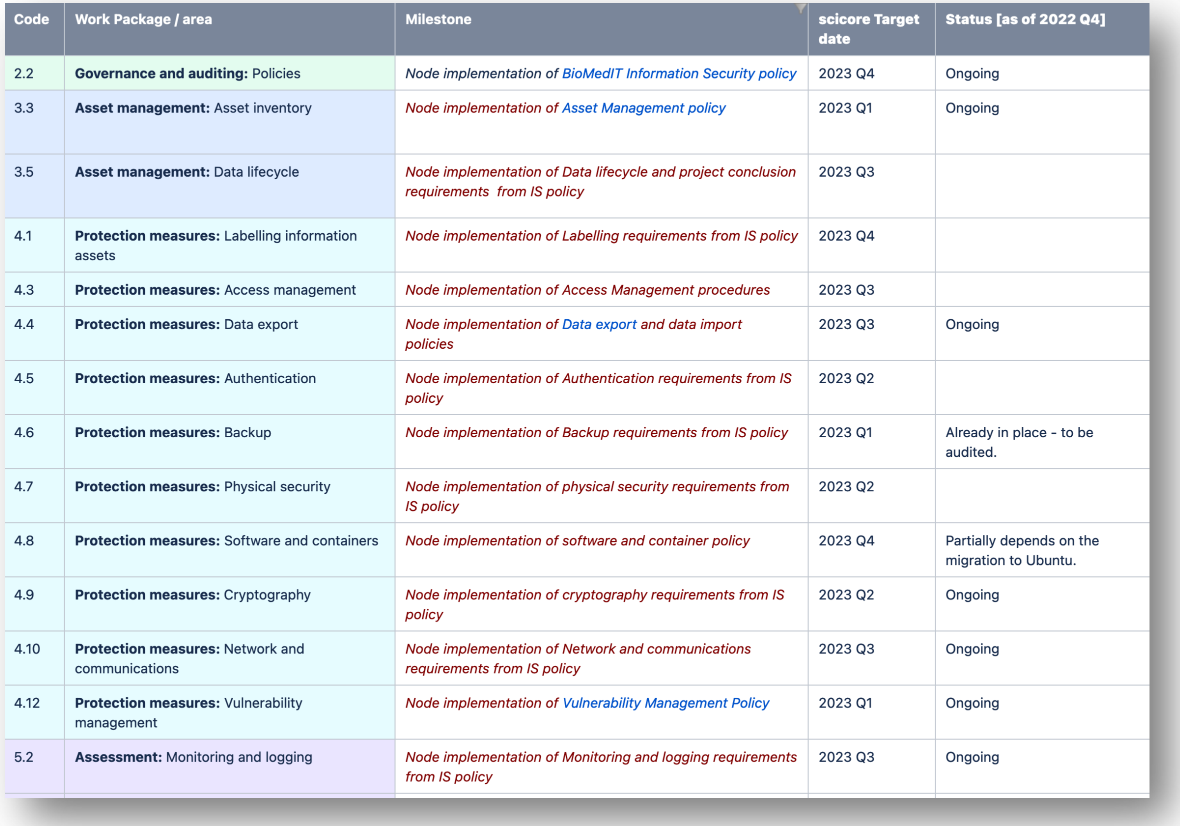
The group is made up of colleagues from across the BioMedIT Network, and is coordinated and chaired by the Personalized Health Informatics (PHI) Group.

Owen Appleton	Sudershan Lakshmanan	Christian Bolliger	Cristian Bovino	Lou Ruppert	Shubham Kapoor
Chair	Member	Member	Member	Member	PHI Representative
PHI, SIB	sciCORE, University of Basel	SIS, ETH Zurich	SIS, ETH Zurich	SIB	PHI, SIB
✉					

https://www.biomedit.ch/

Annual Security Roadmaps

- Achievements and overdues
- Targets
- Priorities
- Deadlines

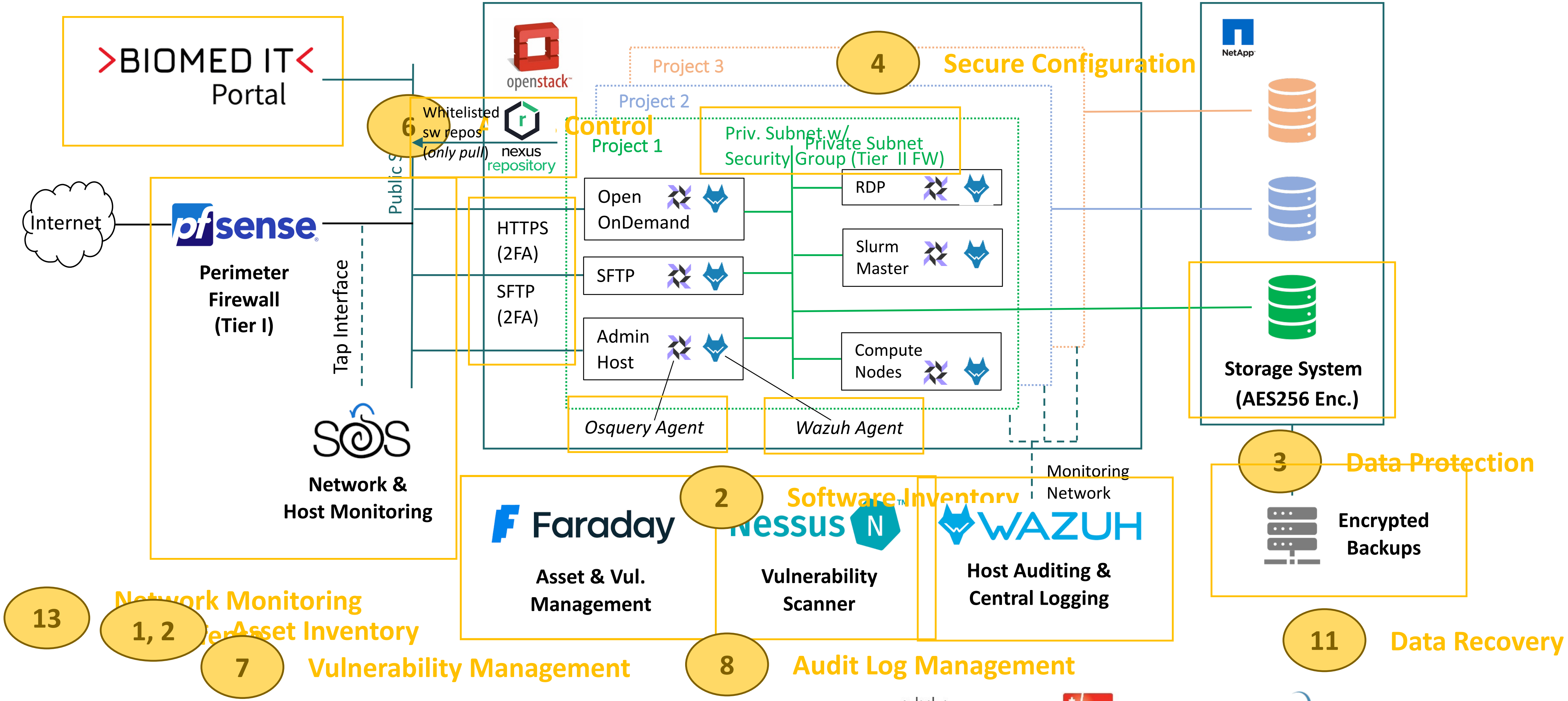


Code	Work Package / area	Milestone	scicore Target date	Status [as of 2022 Q4]
2.2	**Governance and auditing:** Policies	*Node implementation of BioMedIT Information Security policy*	2023 Q4	Ongoing
3.3	**Asset management:** Asset inventory	*Node implementation of Asset Management policy*	2023 Q1	Ongoing
3.5	**Asset management:** Data lifecycle	*Node implementation of Data lifecycle and project conclusion requirements from IS policy*	2023 Q3	
4.1	**Protection measures:** Labelling information assets	*Node implementation of Labelling requirements from IS policy*	2023 Q4	
4.3	**Protection measures:** Access management	*Node implementation of Access Management procedures*	2023 Q3	
4.4	**Protection measures:** Data export	*Node implementation of Data export and data import policies*	2023 Q3	Ongoing
4.5	**Protection measures:** Authentication	*Node implementation of Authentication requirements from IS policy*	2023 Q2	
4.6	**Protection measures:** Backup	*Node implementation of Backup requirements from IS policy*	2023 Q1	Already in place - to be audited.
4.7	**Protection measures:** Physical security	*Node implementation of physical security requirements from IS policy*	2023 Q2	
4.8	**Protection measures:** Software and containers	*Node implementation of software and container policy*	2023 Q4	Partially depends on the migration to Ubuntu.
4.9	**Protection measures:** Cryptography	*Node implementation of cryptography requirements from IS policy*	2023 Q2	Ongoing
4.10	**Protection measures:** Network and communications	*Node implementation of Network and communications requirements from IS policy*	2023 Q3	Ongoing
4.12	**Protection measures:** Vulnerability management	*Node implementation of Vulnerability Management Policy*	2023 Q1	Ongoing
5.2	**Assessment:** Monitoring and logging	*Node implementation of Monitoring and logging requirements from IS policy*	2023 Q3	Ongoing

Security at sciCOREmed

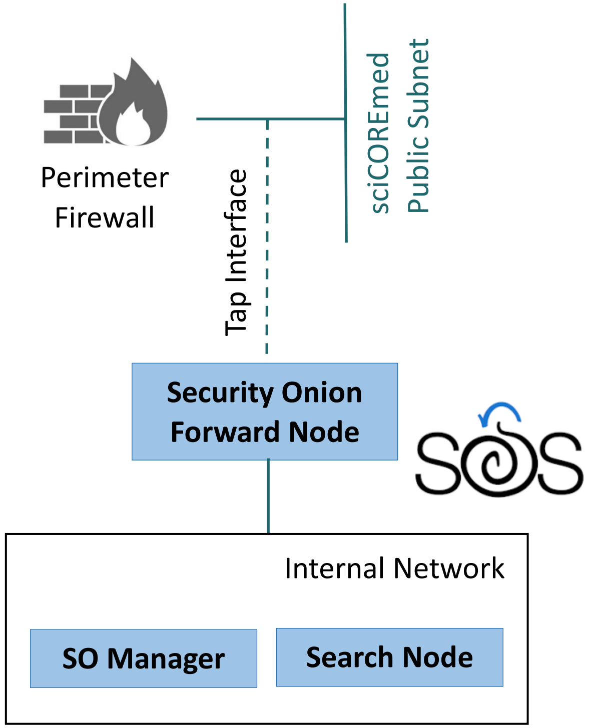
Security at sciCOREmed

sciCOREmed Security Architecture



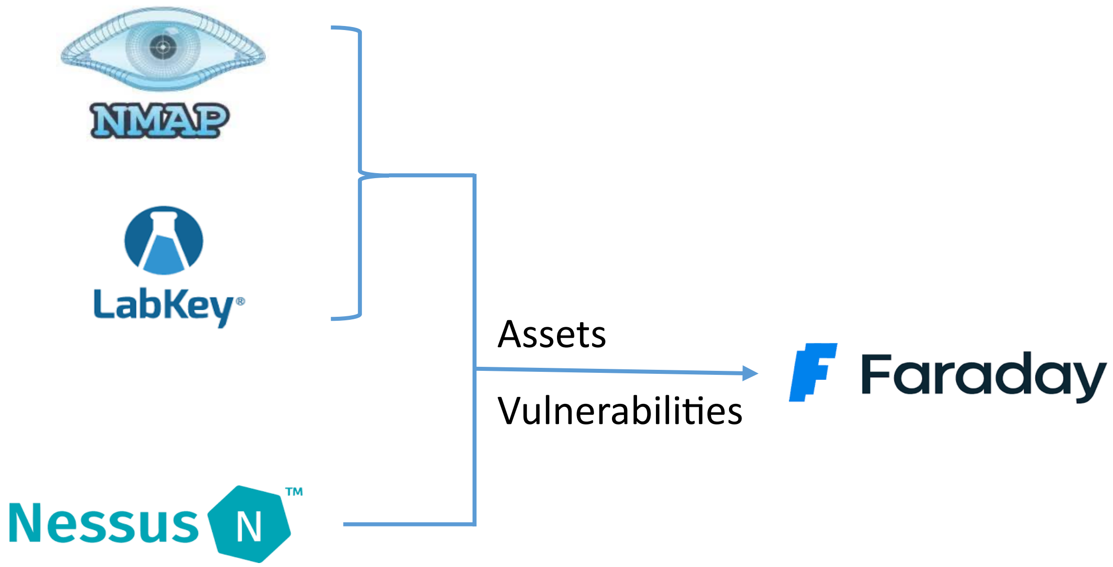
Network Security Monitoring

- A collection of open source tools with traffic monitoring, detecting, and alerting capabilities
- Zeek for traffic monitoring
- Snort and suricata for intrusion detection
- Stenographer for packet capture
- FleetDM/Osquery for device management
- CIS control 13 - Network Monitoring



Asset & Vulnerability Management

- Active asset discovery
- Administrative asset data
- Follows an inventory specification
- Continuous vulnerability scanning
- CIS controls
  - 1, 2 - Asset Inventory
  - 7 - Vulnerability Management

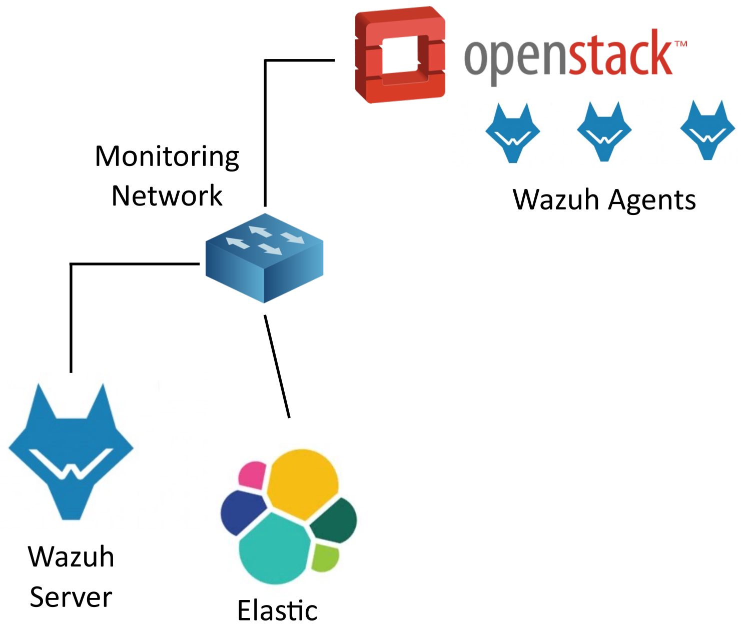


Assets

Vulnerabilities

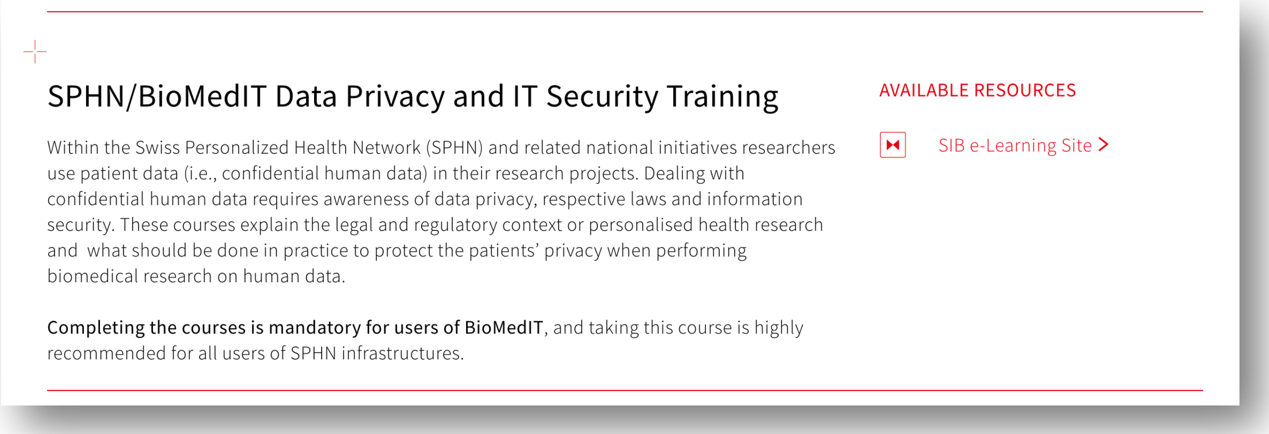
Host Monitoring

- Distributed deployment
- A dedicated VLAN for tenant monitoring
- Monitoring system calls - Auditd/Falco
- Central logging system:
  - tenant VMs
  - management machines
  - firewall logs
- Vulnerability detection - not good
- CIS control 8 - Audit Log Management



Security Training

- Mandatory security training for BioMedIT users
- Recommendations of how to work with sensitive data and legal implications
- Staff training
- CIS Control 14 - Security Awareness and Skills Training



SPHN/BioMedIT Data Privacy and IT Security Training

Within the Swiss Personalized Health Network (SPHN) and related national initiatives researchers use patient data (i.e., confidential human data) in their research projects. Dealing with confidential human data requires awareness of data privacy, respective laws and information security. These courses explain the legal and regulatory context or personalised health research and what should be done in practice to protect the patients' privacy when performing biomedical research on human data.

Completing the courses is mandatory for users of BioMedIT, and taking this course is highly recommended for all users of SPHN infrastructures.

AVAILABLE RESOURCES

SIB e-Learning Site >

https://www.biomedit.ch/home/outreach-training/training.html

Penetration Testing

- Conducted by a third-party company
- Both external and internal services
- Security architecture review, review of firewall rules and exploitation
- An isolated OpenStack tenant simulating real services
- CIS Control 18 - Penetration testing

Ongoing/Future Work

- Vulnerability management - Rapid7 Nexpose
- Asset management, patch management and min. security standards with Ubuntu
- Adopting security controls to sciCORE HPC cluster
- Falco for container runtime monitoring
- Security Onion discontinuing support for Ubuntu, Wazuh and FleetDM/Osquery

Acknowledgements

- sciCORE colleagues
  scicore.unibas.ch/about-scicore/people/

- BioMedIT
  https://www.biomedit.ch

Questions?

References & Additional Resources

sciCOREmed
https://scicore.unibas.ch/projects/scicoremed/

BioMedIT Security
https://www.biomedit.ch/home/biomed-it-infrastructure/security-resources.html

CIS Controls for Effective Cyber Defense
https://www.tml.org/DocumentCenter/View/71/The-CIS-Critical-Security-Controls-Effective-Cyber-Defense-PDF

CIS Controls v8
https://www.cisecurity.org/controls

Control Mappings and Policy Templates
https://www.cisecurity.org/insights/white-papers

CIS CSAT
https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat_pre