Cr-des Project

CYBERSECURITY VIRTUAL LAB AS A SERVICE

Vipuvoimaa EU:lta 2014–2020

Vaasan yliopisto
UNIVERSITY OF VAASA

Structure

SERVICE DESCRIPTION

SERVICE ARCHITECTURE

VALUE PROPOSITION

SERVICE ECOSYSTEM

Service Description

DESCRIBES:

- The strategic plans
- Governance structure
- Risk management plans
- Processes that will be used to create business outcomes, deliver services and create value

Strategy and Planning

- Vision
- 1. Develop and Create solutions-based cyber security services for smart grids nationally and internationally.
- 2. Build cyber security human capabilities through training and research.

- Mission
- 1. Provide real-time information on current and emerging security threats and vulnerabilities for smart grids.
- 2. Commercialize the simulation platform into paid service products.
- 3. Implementation of new R&D projects.

Vaasan yliopisto
UNIVERSITY OF VAASA

Strategy and Planning (Cont.)

Goals	Description
Real-Time Simulation	Develop Testing and Real-time scenarios on security threats.
Training	Provide Training Services for security professionals
Research and Development	Provide a Platform for further R&D

Governance Structure

Steering and Technical committee to manage the virtual laboratory's operations and guide decision-making

Service Strategy

- Workplan Preparation, Monitoring, and Control
- Enterprise Architecture
- Project Governance and Management

Service Design

- Workplan Preparation, Monitoring, and Control
- Procurements and Contract Management

Service Delivery

Project Governance and Management

Life cycle Management

Service Operations

Service Management

Security Management

Service Validation and Testing

Integration with Service Design

Service quality and assurance

Testing strategies

Test models, approaches and techniques

Vaasan yliopisto
UNIVERSITY OF VAASA

Service Strategy

Work program to define objectives, activities, expected results, performance indicators, and related human and financial resources

Strategy for identifying and integrating new and emerging technologies

Vaasan yliopisto
UNIVERSITY OF VAASA

Service Design

- The work program to plan and organize resources, such as physical or digital artifacts, developers and customers, workflows, and procedures

SERVICE DESIGN PROCESS

- Service Requirements
- Service Offerings
- Service Agreements
- Service Delivery

Service Requirements

- Requirement Capabilities
- Requirement Management
- Management Responsibilities
- Requirements Architecture
- Architecture Responsibilities
- Requirements Team

- Requirements Capabilities: Collect functional and non-functional, physical, service offerings, cost, risk management, service delivery, agreements, and service validation requirements.
- Requirements Management: Ensures that the management and capabilities are controlled, balanced, and aligned with the mission and needs.
- Requirements Architecture: Ensure feasibility in terms of Requirements Capabilities
- Architecture Responsibilities: Providing service architecture concepts, descriptions, models, viewpoints, specifications, and analyses
- Requirements Team: Handles integration, data, configurations, records, information utilization, and system requirements

Service Offerings

REAL-TIME CO-SIMULATION SCALABLE EXATACPS AND HYPERSIM OPAL-RT

CPS TESTING SCENARIOS THAT PROVIDE A HANDS-ON DEMONSTRATION OF THE IMPACT OF MODP

CPS TESTING SCENARIOS THAT ASSESS OFFENSIVE ASPECTS OF THE CYBERSPACE

CLOUD-BASED LABS

Vaasan yliopisto
UNIVERSITY OF VAASA

Determination of free service subscription (Suggestions)

LEVEL OF ACCESS: LIMITED ACCESS TO THE VIRTUAL LAB OR A SPECIFIC SET OF SERVICES

SERVICES OFFERED: BASIC SERVICES OR A LIMITED SET OF FEATURES OF THE PAID SERVICES

TIME LIMIT: A TRIAL PERIOD OF A FEW DAYS OR WEEKS, OR AN ONGOING SUBSCRIPTION WITH LIMITED ACCESS

DATA LIMITATIONS:LIMITS ON THE AMOUNT OF DATA THAT CAN BE PROCESSED, STORED OR ANALYZED

UPGRADES AND UPSELLS:UPGRADE TO PAID SERVICES AND WHAT ADDITIONAL FEATURES AND BENEFITS ARE AVAILABLE

Vaasan yliopisto
UNIVERSITY OF VAASA

Productization of paid services (suggestions)

- Service Tiers: Different tiers of services, such as levels of support, response times, or data processing capabilities
- Pricing Model: Charging based on usage, subscription-based pricing, or project-based pricing
- Marketing and Sales: Digital marketing campaigns, targeted advertising, webinars, or networking with potential clients.
- Customer Support: Support through multiple channels, such as phone, email, and chat(e.g., Chatbots)
- Scalability: Ensure that the paid services can be scaled as the demand grows

Service Agreement

- Service agreements with all stakeholders and partners to determine:
- The scope of services
- Service level objectives
- Pricing
- Terms and conditions

Service Delivery

- Service request management
- Incident management
- Change management
- Service Metrics and Reporting
- Security Management
- Risk Management Plan

Risk Management Plan

The risk management plan informs teams of the steps they must take to identify, analyze, and respond to all risks that may affect the cyber security virtual

Potential Risks	Severity of Risk	Mitigation Strategies
Unauthorized Access	High	Data Encryption: Data encryption should be implemented on all sensitive data to protect it from unauthorized access
Data Breaches	High	Regular Backups: Regular backups should be performed to ensure that data can be restored in case of data breach.
Software Vulnerabilities	High	Vulnerability Scanning: Regular vulnerability scanning and testing should be performed in the virtual laboratory to identify vulnerabilities in the system
Malware and Ransomware Attacks	High	Use Antivirus and Antimalware Software, Regularly Update Software and Operating Systems, Implement Firewall Protection, and Limit User Access.
Insufficient User Authentication and Authorization	High	Access Controls: Implement a strong access control policy that includes strong passwords, two-factor authentication, and regular password changes
Physical Damage	Low	Implement physical security such as access control, surveillance cameras, and alarms, Regular Maintenance

- Responsible Team: Incident response team
- Response Plan: Identify and Contain the Incident, Investigate the Incident, Notify Law Enforcement and Affected Parties, Restore Operations, Review the incident
- Communication Plan: Identify Stakeholders, and inform them about the incident, the potential impact, and actions that need to be taken via email, phone, social media, or press releases.

Service Validation and Testing

The goal is to ensure that the services associated with the cyber-security platform are of the required quality.

Ensure Integration with service design

Service quality assurance

Testing strategies

Test models, approaches and techniques

Categories of Users and Subscription Plans

Customers/Clients	Services	Subscription
Students	Cyber Security Exercises	Free Subscription
Researchers	Research and Development	Free/Paid Services
Security Professionals	Training, Simulations	Paid Services
Organizations	Testing, Training, Projects, Simulations	Paid Services

Testing methods

SERVICE TESTING

Test	Purpose
Unit testing	For testing individual methods and functions of the classes, components, or modules used by the virtual lab
Integration tests	Verify that different modules or services used by virtual labs work well together. E.g., testing the interaction with the database or making sure that microservices work together as expected
Functional tests	Focus on an application's business requirements in verifying an action's output.
Performance testing	Evaluates how a system performs under a particular workload. These tests help measure the virtual lab's reliability, speed, scalability, and responsiveness.
End-to-end tests	Replicates a user behavior with the software in a complete application environment. It verifies that various user flows work as expected. For example, logging in or more complex scenarios verifying email notifications, online payments, etc.

Methods	Description
Endpoint Detection and Response (EDR)	Testing to simulate insider threats for smart grids to assess businesses' abilities to recognize and respond to malicious acts by trustworthy insiders. This test monitors and defends endpoints against sophisticated threats and attacks on Intelligent Electronic Devices (IEDs), smart metering systems, Substation Automation Systems (SAS), Communication Gateways, and Control Center Systems. EDR tests are designed to identify, investigate, and respond to abnormal endpoint activity in real time.
Security Information and Event Management (SIEM)	This method will replicate the centralization of security event data collecting, analysis, and correlation from diverse sources within a system or network. In the context of smart grids, SIEM is critical for monitoring and handling security incidents to protect the grid's infrastructure and data's integrity, availability, and confidentiality.
User and Entity Behavior Analytics (UEBA)	This method analyzes the behavior patterns of users and entities within a system or network to detect anomalies, identify potential insider threats, and mitigate security risks. Using UEBA to simulate insider threats in a cyber security virtual laboratory for smart grids can help organizations assess the effectiveness of their UEBA solutions in detecting and responding to insider threats.
Insider Threat Management (ITM)	This method entails the techniques, tools, and strategies businesses use to detect, prevent, and respond to insider threats. Using ITM to simulate insider threats in a cyber security virtual laboratory for smart grids can assist organizations in assessing their ITM capabilities and readiness to cope with such attacks. In the virtual lab, SCADA systems, smart meters, and communication devices can be modeled to

Simulation testing

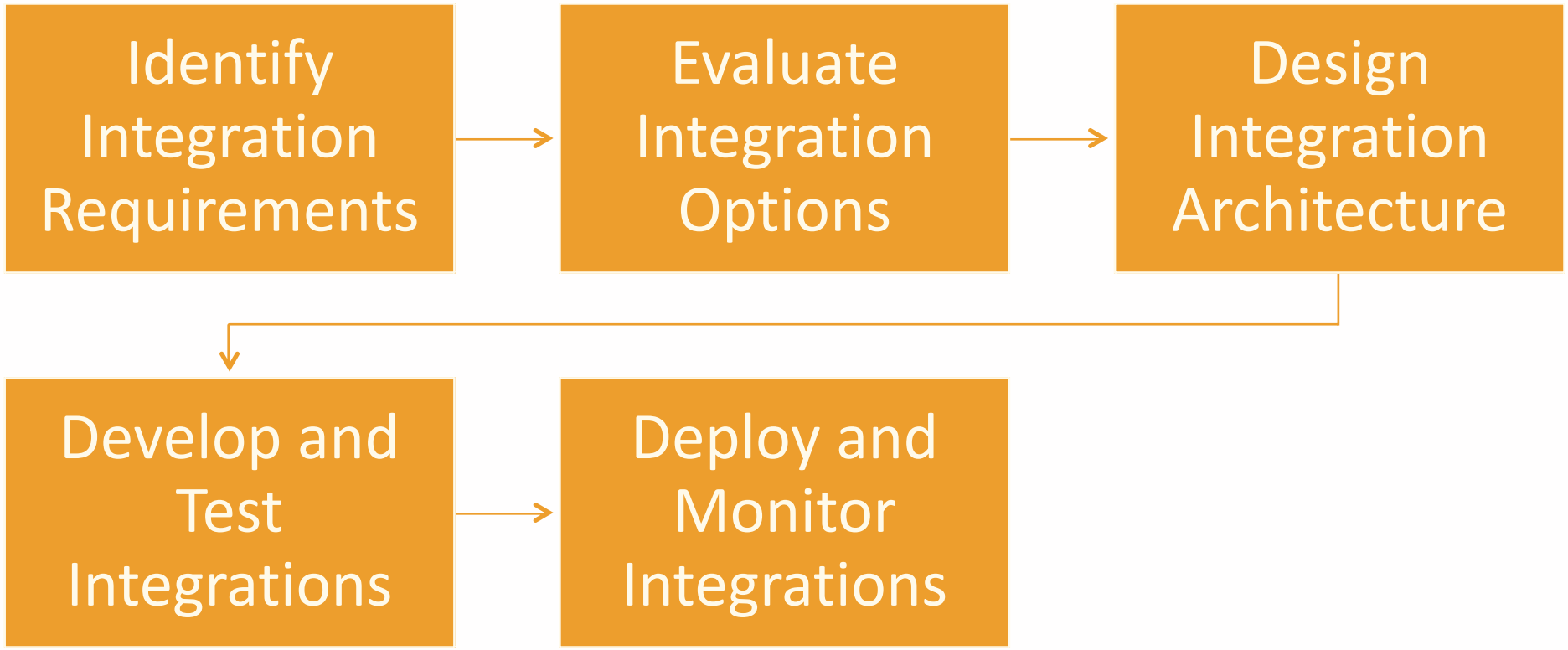
Through our service offerings, the virtual lab will simulate how resilient smart grids and critical infrastructure can perform and deal with all potential threats, such as cyber-attacks, Insider threats, and equipment failure.

Vaasan yliopisto
UNIVERSITY OF VAASA

Testing Plan

Steps	Description
Determine the Test Scope	Decide on the type, services, and parameters for testing
Define the Test Cases	Design test cases to cover and identify a wide range of scenarios and potential issues and bugs
Identify Testing Tools	Decide on the testing tool
Develop Testing Procedures	Decide on the steps, data to be collected, and expected outcomes
Conduct Testing	Perform the actual tests
Analyze Results	Identify bugs and issues found, document and prioritize according to the urgent need for a solution.
Address Issues	Fix the issues, make necessary changes, and re-test.

Integration plan



Vaasan yliopisto
UNIVERSITY OF VAASA

Value Proposition

Target Group	Value Proposition
Energy Companies and Other Organizations	• Improved cyber resilience • Cost-effective testing • Research and Development • Training and Support
Researchers and Students	• Real-world simulation • Accessibility • Cost-effective • Collaboration
Security Professionals	• Realistic simulation • Comprehensive training • Risk-free experimentation • Cost-effective • Collaboration

Service Architecture

FRONT-END INTERFACE

SIMULATION ENGINE

DATA MANAGEMENT SYSTEM

REPORTING AND ANALYSIS MODULE

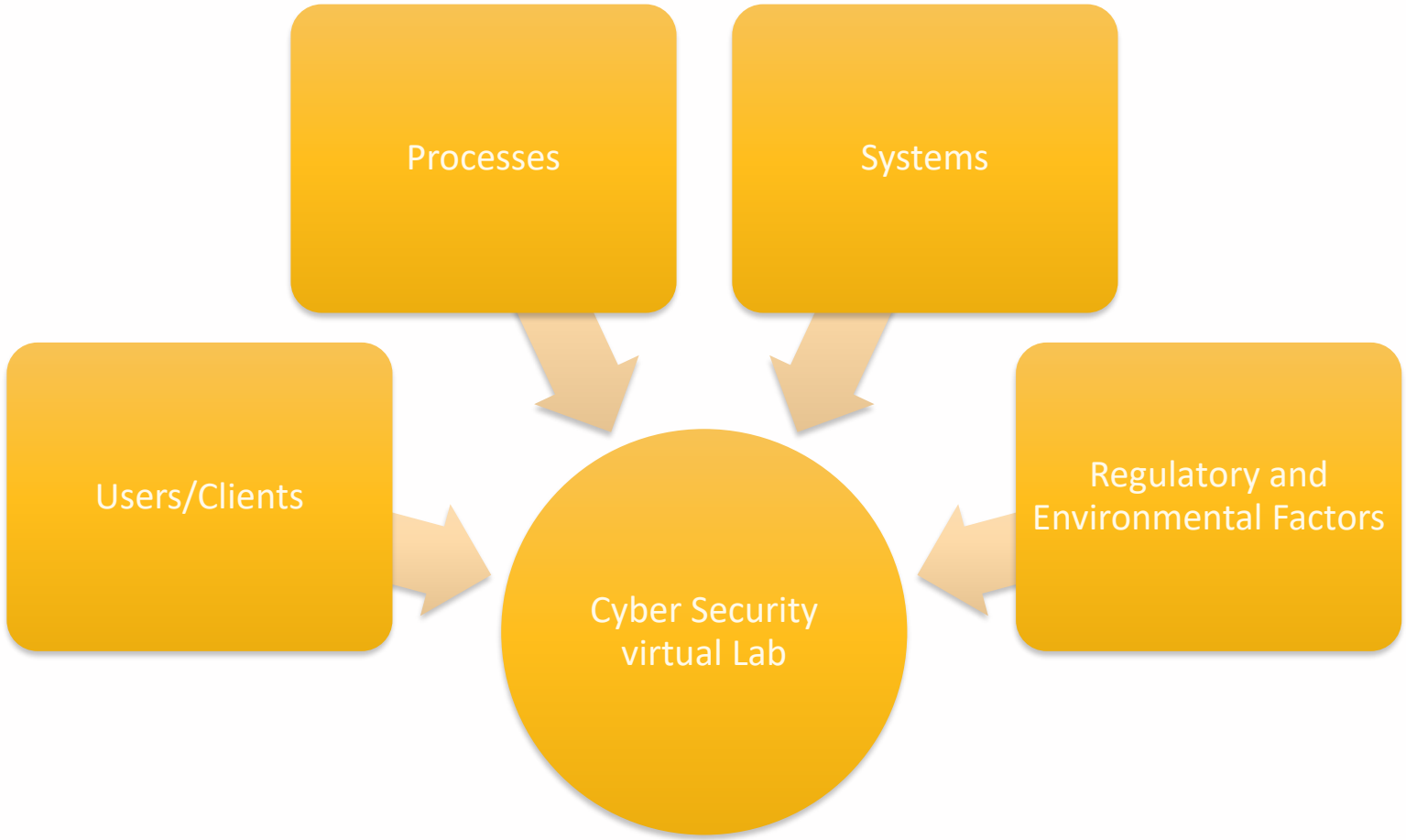
SECURITY CONTROLS

INTEGRATION WITH SMART ENERGY GRIDS

MAINTENANCE AND SUPPORT:

Vaasan yliopisto
UNIVERSITY OF VAASA

Service Ecosystem



Vaasan yliopisto
UNIVERSITY OF VAASA

New R&D Ideas

As cyber threats and attacks become increasingly complex, there are various research and development areas available through cyber security virtual laboratories to assist organizations, academics, and security professionals in improving their cyber security capabilities. Some of these ideas are as follows:

- Blockchain Security: Applying blockchain has the potential to be a dominant tool in cybersecurity since it provides better methods of protection and greater flexibility
- Incorporating artificial intelligence and machine learning algorithms into a virtual laboratory can increase danger identification, response accuracy, and speed.
- The convergence of IoT with Smart Grids allows real-time data collection from all network locations.
- With the expansion of IoT devices, a virtual laboratory that can simulate IoT-based threats and evaluate IoT security measures is required. This can assist enterprises in ensuring the security of their IoT devices and networks.

The Future of The Cyber Security Virtual Laboratory

A mix of technology breakthroughs, increasing cyber threats, and changing organizational needs will influence the future of the cyber security virtual laboratory. The following are some potential advancements that could shape the future of the cybersecurity virtual laboratory

- Improved capabilities for more advanced simulation
- Integration with Artificial Intelligence and Machine Learning
- Increased Integration with the Cloud and IoT
- Improved Visualization and Analytics
- Greater Collaboration and Information Sharing
- Increased Focus on Training and Education

References

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: Https://Nvlpubs. Nist. Gov/Nistpubs/CSWP/NIST. CSWP, 4162018.

Director Consultation Groups – Core Business IT Target Operating Model 2023—2027. (n.d.).

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., Wollman, D., & others. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0. Department of Commerce. National Institute of Standards and Technology

Hassan, F. (2010). The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18–28.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25.

Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews, 59, 710–725. https://doi.org/10.1016/j.rser.2016.01.011

Tuunainen, V. K., & Tuunanen, T. (2011). IISIn-A model for analyzing ICT Intensive Service Innovations in n-sided Markets. 2011 44th Hawaii International Conference on System Sciences, 1–10.

Tuunanen, T., Bask, A., & Merisalo-Rantanen, H. (2012). Typology for modular service design: Review of literature. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 3(3), 99–112.

Tuunanen, T., Myers, M. D., & Cassab, H. (2010). A conceptual framework for consumer information systems development. Pacific Asia Journal of the Association for Information Systems, 2(1), 5.

Williams, K., Chatterjee, S., & Rossi, M. (2008). Design of emerging digital services: A taxonomy. European Journal of Information Systems, 17(5), 505–517.