Iniciada	sábado, 20 de janeiro de 2024 às 10:01
Estado	Terminada
Terminada	sábado, 20 de janeiro de 2024 às 11:55
Tempo gasto	1 hora 53 minutos
Nota	**17,00** num máximo de 20,00 (**85**%)

Informação

[PT]

O pessoal da EDP pretende ter acesso a um portal quando estão quer na empresa quer no terreno a efectuar instalações, manutenções ou a corrigir problemas.

Neste contexto, o SecureSmartMeter foi contratado à tua empresa.

Ficará em https://securesmartmeter.pt e será apenas acessível para funcionários credenciados da EDP e os subempreiteiros da EDP que efetuam trabalhos no terreno.

O que se pretende com este portal é dar, em tempo real, acesso às informações de todo e qualquer Smart Meter de energia da rede da EDP, o portal deve permitir o acesso aos detalhes do Smart Meter (configurações, estado, versões, consumo actual, hora, última actualização, detalhes do utilizador do serviço ...).

Esta informação deve ser complementada pela informação de histórico de cada Smart Meter que está cebtralizada na EDP. Esta informação, acessível por internet através de um interface que pode ser explorado por webservices, existe em duas bases de dados redundantes e contém o histórico de consumos, pagamentos, utilizações, alterações e manutenções, alarmes e outras operações associadas a cada Smart Meter.

Se o primeiro caso é, geralmente mais interessante para os funcionários que se deslocam ao terreno, a segunda base de dados não é menos interessante pois apresenta tendências de consumo, e pode permitir a identificação de utilização fraudulenta dos equipamentos. Estes dados ficam registados sem encriptção pois a EDP pretende correr aplicações de monitorização permanente de fraude e que exigem muito processamento não podendo suportar encriptação, estas aplicações devem ser intergradas no SafeSmartMeter e deves também implementar o envio de mensagens (email configurável) quando uma certa tendência ou um alarme de fraude for detectado.

Há ainda, estranhamente, um requisito pedido a possibilidade de fazer o reset aos dados de um deteminado Smart Meter pelo funcionário (sem mais restrições para este reset), para reíniciar um serviço com um novo cliente ou para corrigir problemas com determinado Smart Meter – A tua empresa tem levantado dúvidas relativamente a esta funcionalidade, que apenas de ficar registado quem efectuou o reset dos dados, os mesmos acabam por ficar perdidos para sempre, podendo levar a situações fraudulentas camufladas.

It will be located at https://securesmartmeter.pt and will only be accessible to accredited EDP employees and EDP subcontractors carrying out work on the ground.

The aim of this portal is to provide, in real time, access to information from each and every energy Smart Meter on the EDP network. The portal must allow access to the details of the Smart Meter (settings, status, versions, current consumption , time, last update, service user details...). This information must be complemented by the historical information of each Smart Meter that is centralized at EDP. This information, accessible via the internet through an interface that can be explored by web services, exists in two redundant databases and contains the history of consumption, payments, use, changes and maintenance, alarms and other operations associated with each Smart Meter.

If the first case is generally more interesting for employees who travel to the field, the second database is no less interesting as it presents consumption trends, and can allow the identification of fraudulent use of equipment. This data is recorded without encryption as EDP intends to run permanent fraud monitoring applications that require a lot of processing and cannot support encryption. These applications must be integrated into SafeSmartMeter and you must also implement the sending of messages (configurable email) when a certain trend or a fraud alarm is detected.

There is also, strangely, a requirement for the possibility of resetting the data on a specific Smart Meter by the employee (with no further restrictions for this reset), to restart a service with a new customer or to correct problems with a specific Smart Meter – Your company has raised doubts regarding this functionality, because it is only recorded who reset the data, and data ends up being lost forever, which could lead to camouflaged fraudulent situations.

Informação

[PT] (English Version follows below)

As respostas podem ser redigidas em Português ou em Inglês.

É natural que a descrição da solução seja omissa e que não contenha todos os detalhes para a implementação da mesma, para isso seria necessário um caderno de encargos que poderia demorar horas a ler. Se for necessária mais informação para responder a uma ou mais perguntas podes **definir pressupostos** desde que realistas e aplicáveis à situação.

A consulta do material fornecido em aulas é permitida.

O exame apresenta uma pergunta por página para evitar a perda de informação se houver problemas, nas perguntas relacionadas com as anteriores é possível navegar sem restrições e aconselhável fazer a cópia da resposta anterior para servir de base à próxima resposta. Podes efectuar a resposta à parte e depois copiar para o Moodle. É aconselhável gravar as respostas com alguma frequência,

É sugerido leres de novo a pergunta depois de respoderes para te certificares que respondeste a tudo o que é pedido.

Nota: Quando se refere a atributos o atributos de seguança é o mesmo que os "security goals", por exemplo Confidencialidade, Integridade, Disponibilidade, etc.

O Exame tem uma duração de 2 horas, ao fim das quais o mesmo ficará bloqueado e o sistema submeterá as respostas introduzidas na altura.

Boa sorte!

[EN]

Answers can be written in Portuguese or English.

It is natural that the description of the solution is incomplete and does not contain all the details for its implementation, for this reason it would be necessary to have specifications that could take hours to read. If more information is needed to answer one or more questions, you can

can answer separately and then copy it to Moodle (advised). It is advisable to record responses frequently.

It is suggested that you read the question again after answering to make sure you have answered to everything asked.

Note: When referring to attributes, security attributes are the same as "security goals", for example Confidentiality, Integrity, Availability, etc.

The Exam lasts 2 hours, after which it will be blocked and the system will submit the answers entered at the time.

Good luck!

Pergunta **1**

Respondida

Nota: 2,00 em 2,00

[PT]

a) Lista 3 razões pelas quais, para este projecto em específico, é importantíssimo considerar a formação da equipa de projecto na área de cibersegurança e efectuar análises de "Threat Modelling" (dando, por exemplo, um exemplo para cada razão).

b) Identifica 3 tópicos (assuntos) que deveriam fazer parte do Processo de Resposta a Incidentes que deve ser definido no final do projecto.

[EN]

a) List 3 reasons why, for this specific project, it is extremely important to consider training the project team in the area of cybersecurity and carry out "Threat Modeling" analyzes (giving, for example, an example for each reason).

b) Identify 3 topics (subjects) that should be part of the Incident Response Process that must be defined at the end of the project.

a) É de extrema importância considerar a formação da equipa de projeto na área de cibersegurança e efetuar análises de "Threat Modelling", pois:

1. Os requisitos de segurança têm de ser muito bem definidos, pois este portal trabalha com informação sensível que envolvem operações sobre dados que podem afetar a integridade do sistema.
2. A equipa do projeto tem de tomar em conta na sua implementação a situação onde um funcionário é vítima de uma campanha de phishing, de modo a ter um sistema mais seguro a falsificação de identidade.
3. A equipa tem de ter em conta na sua implementação, um modo de combater ataques de negação de serviço, pois este portal tem que estar sempre ativo para que os funcionários que não se encontram no terreno possam fazer as devidas manutenções.

b) No processo de resposta a incidentes, deve ser definido:

2. Gestão de Logs e Auditoria: Implementar um sistema robusto de logs que registe todas as ações realizadas no portal, incluindo resets de dados. Desenvolver procedimentos para revisão periódica de logs e auditorias internas para identificar padrões incomuns que possam indicar atividades fraudulentas.
3. Resposta a Incidentes de Fraude: Estabelecer um protocolo claro para responder a incidentes de fraude detetados, incluindo a comunicação rápida com as partes interessadas, a revisão detalhada das atividades suspeitas e a implementação de medidas corretivas, como o bloqueio de acessos ou a revogação de privilégios de reset de dados.

Comentário:

Pergunta **2**

Respondida

Nota: 2,25 em 3,00

[PT]

Considerando uma análise de ameaças de segurança (threats analysis) aplicável a este sistema:

a) Identifica os principais atributos de segurança que se devem ter em conta neste caso (o que é mais importante), e explica brevemente cada um deles com um exemplo para cada um (3 atributos no mínimo, 6, no máximo). Considera pelo menos os atributos CIA.

b) Dá um exemplo de como se poderia monitorizar a Disponibilidade do sistema de forma eficaz. (Podes apresentar uma proposta de solução, arquitectura ou procedimentos...)

c) Identifica uma vulnerabilidade (genérica) que poderia ser analizada para as possíveis tecnologias envolvidas.

[EN]

Considering a security threat analysis applicable to this system:

a) Identify the main security attributes that must be taken into account in this case (which are the most important), and briefly explain each of them with an example for each one (3 attributes minimum, 6 maximum). Consider at least the CIA attributes.

b) Give an example of how system Availability could be monitored effectively. (You can present a proposal for a solution, architecture or procedures...)

c) Identify a (generic) vulnerability that could be analyzed for the possible technologies involved.

a) Os principais atributos de segurança são:

1. Confidencialidade**:** Garante que apenas as partes autorizadas tenham acesso a informações sensíveis. Pois na gestão do histórico do

acesso de dados, ajuda a garantir a integridade dos dados.

3. Disponibilidade**:** Garante que os serviços e dados estejam disponíveis quando necessário, sem interrupções indevidas. A disponibilidade é crucial para garantir que os funcionários da EDP acessem o portal SecureSmartMeter em tempo real durante instalações ou manutenções. Medidas como redundância de servidores, sistemas de backup e planos de recuperação de desastres garantem a disponibilidade contínua do sistema, mesmo em situações adversas.

b) Implementar um sistema de balanceamento de carga para distribuir o tráfego entre servidores e granularidade nas bases de dados. Além disso, utilizar servidores redundantes e configurar failovers garante que, se um servidor falhar, o tráfego seja automaticamente redirecionado para um servidor funcional, minimizando o impacto. Utilização de sistemas de deteção de intrusão (IDS) de modo a procurar por anomalias no portal, como interseções de informação (pois os dados presentes nas bases de dados não se encontram cifrados), e definição de regras no firewall do portal.

c) Uma vulnerabilidade que poderia ser analisada dentro deste âmbito, seria SQLi (SQL injection), dado à importância dos dados do mesmo e do facto de eles encontrarem-se armazenados em texto limpo.

Comentário:
a) OK

b) " monitorizar a Disponibilidade do sistema" - tu dás uma solução genérica de load balancing, redundânia, e detecção de intrusões, mas quanto à monitorização de disponibilidade pouco referes.

c) OK

Pergunta **3**

Respondida

Nota: 3,00 em 3,50

[PT]

A FMEA é uma técnica para analisar concretamente modos de falha, e quais seriam as causas, efeitos, o método de detecção e possíveis alterações ao sistema para reduzir o impacto das falhas individuais.

Para o sistema a desenvolver, identifica 3 funções com impacto na segurança do sistema (por exemplo "Autenticar utilizador", “Fazer o log de operações críticas”, “emitir um alarme”) e analisa **para cada função**, com os modos de falha básicos (função não executada, função tardiamente executada e função mal executada), quais seriam:

- Possíveis métodos de detecção das falhas,
- Efeitos previstos se as falhas não forem eliminadas, e
- Uma sugestão para eliminar as falhas ou para controlar os seus efeitos.

(para cada função e para cada modo de falha que leve a um efeito indesejável)

[EN]

The FMEA is a technique for concretely analyzing failure modes, and what the causes, effects, detection method and possible changes to the system would be needed to reduce the impact of individual failures.

For the system to be developed, identify 3 functions with an impact on system security (for example “Authenticate user”, “Log critical operations”, “issue an alarm”) and analyze for each function, with the basic failure modes (function not executed, function late executed and function poorly executed), which would be:

- Possible fault detection methods,
- Expected effects if faults are not eliminated, and

    - Métodos de Deteção: Monitorização de logs de autenticação, alertas para múltiplas tentativas falhadas.
    - Efeitos Previstos: Acesso não autorizado ao sistema, comprometendo a confidencialidade e integridade dos dados.
    - Sugestão de Eliminação/Controlo: Implementação de bloqueios automáticos após um número definido de tentativas falhadas, além de autenticação de dois fatores para camadas adicionais de segurança.
- Modo de Falha 2: Função Tardiamente Executada
    - Métodos de Deteção: Registo de eventos com timestamp para detetar atrasos anormais no processo de autenticação.
    - Efeitos Previstos: Atrasos no acesso ao sistema, possivelmente resultando em frustração do utilizador e aumentando o risco de ataques de força bruta.
    - Sugestão de Eliminação/Controlo: Otimização do processo de autenticação, garantindo tempos de resposta aceitáveis. Implementação de caches de autenticação para reduzir a latência.
- Modo de Falha 3: Função Mal Executada
    - Métodos de Deteção: Análise de logs para identificar padrões de comportamento anormal durante a autenticação.
    - Efeitos Previstos: Autenticação incorreta, permitindo acesso não autorizado ou negando acesso a utilizadores legítimos.
    - Sugestão de Eliminação/Controlo: Melhoria nos algoritmos de autenticação, incluindo a adoção de métodos mais seguros e a validação adequada de entradas.

2. Efetuar o Log do Histórico de Consumo:

- Modo de Falha 1: Função Não Executada
    - Métodos de Deteção: Monitorização proativa dos logs para identificar lacunas nas entradas de histórico.
    - Efeitos Previstos: Perda de dados históricos essenciais para análises de consumo e tendências.
    - Sugestão de Eliminação/Controlo: Implementação de mecanismos de redundância nos logs e processos automatizados para alertar quando ocorrerem lacunas.
- Modo de Falha 2: Função Tardiamente Executada
    - Métodos de Deteção: Comparação entre o timestamp esperado e o timestamp real nas entradas de log.
    - Efeitos Previstos: Atrasos na atualização do histórico, prejudicando a análise em tempo real e a deteção precoce de anomalias.
    - Sugestão de Eliminação/Controlo: Otimização dos processos de log e utilização de técnicas de paralelização para melhorar a eficiência.
- Modo de Falha 3: Função Mal Executada

- Modo de Falha 1: Função Não Executada
    - Métodos de Deteção: Registo de eventos associados ao pedido de reset não processado.
    - Efeitos Previstos: Incapacidade de reiniciar um serviço ou corrigir problemas em Smart Meters, impactando as operações no terreno.
    - Sugestão de Eliminação/Controlo: Implementação de procedimentos de gestão de filas de pedidos para garantir que todos os resets solicitados sejam processados.
- Modo de Falha 2: Função Tardiamente Executada
    - Métodos de Deteção: Comparação entre o timestamp esperado e o timestamp real para o reset.
    - Efeitos Previstos: Atrasos na execução de resets, afetando a eficiência das operações no terreno.
    - Sugestão de Eliminação/Controlo: Otimização do processo de reset e utilização de notificações automáticas para informar sobre o estado do pedido.
- Modo de Falha 3: Função Mal Executada
    - Métodos de Deteção: Monitorização de logs para identificar padrões suspeitos ou resets inesperados.
    - Efeitos Previstos: Possíveis ações fraudulentas ou reinicializações indevidas de serviços.
    - Sugestão de Eliminação/Controlo: Implementação de autenticação adicional para realizar operações sensíveis, além de revisão rigorosa dos logs para identificar atividades suspeitas

Comentário:

1. Autenticar o Utilizador:

- Modo de Falha 1: Função Não Executada
    - Métodos de Deteção: Monitorização de logs de autenticação, alertas para múltiplas tentativas falhadas.
    - Efeitos Previstos: Acesso não autorizado ao sistema, comprometendo a confidencialidade e integridade dos dados.
- Quer o modo de deteção quer os efeitos não estão muito correctos, não será por tentativas falhadas que se detecta a não execuçã ode uma função (se ele não executa...), e o seu efeito será mais a não autenticação de ninguém, caso o principio de failsecure for aplicado

Pergunta **4**

Respondida

Nota: 2,50 em 3,00

[PT]

Descrever 6 requisitos **relacionados com a segurança** funcional do sistema. Caso a descrição do sistema a desenvolver não permita identificar claramente requisitos fazer pressupostos (o cliente na maioria das vezes não faz bem ideia do que precisa, é perfeitamente normal fazer propostas lógicas e com sentido).

Para cada requisito identificar quais os **atributos de segurança** que estão relacionados, garantido que existe pelo menos um requisito relacionado com o atributo "Integridade/Integrity".

[EN]

Describe 6 requirements related to the functional safety of the system. If the description of the system to be developed does not allow you to clearly identify requirements, make assumptions (the client most of the time has no idea what they need, it is perfectly normal to make logical and meaningful proposals).

For each requirement, identify which security attributes are related to it, ensuring that there is at least one requirement related to the "Integrity" attribute.

REQ-01: O sistema deve garantir a integridade dos dados armazenados, processados e transmitidos, prevenindo alterações não autorizadas. Isso inclui a proteção contra qualquer forma de corrupção, manipulação ou destruição não autorizada dos dados.

- Atributos de Segurança Relacionados: Integridade, Autenticidade.

REQ-02: O sistema deve atribuir e gerir de forma responsável as permissões e acessos, assegurando que cada utilizador tem apenas as autorizações necessárias para realizar as suas funções. Isso inclui a capacidade de revogar rapidamente privilégios de utilizadores que não

REQ-04: O sistema deve garantir a disponibilidade contínua dos serviços críticos, minimizando o tempo de inatividade e assegurando que os utilizadores autorizados tenham acesso ao sistema quando necessário.

- Atributos de Segurança Relacionados: Disponibilidade, Continuidade de Serviço.

REQ-05: O sistema deve manter registos detalhados de todas as atividades relevantes, incluindo autenticações, alterações de permissões e eventos críticos. Estes registos devem ser monitorizáveis, de modo a permitir a deteção de comportamentos anómalos ou tentativas de violação.

- Atributos de Segurança Relacionados: Integridade, Auditoria, Não Repúdio.

REQ-06: O sistema deve ter procedimentos claros e eficazes para a resposta a incidentes de segurança. Isso inclui a identificação, análise e mitigação rápida de incidentes, bem como a comunicação transparente com as partes interessadas.

- Atributos de Segurança Relacionados: Disponibilidade.

Comentário:
REQ-2 O que é uma forma responsável?

Pergunta **5**

Respondida

Nota: 2,25 em 3,50

[PT]

Definir um conjunto de testes (sob a forma de uma especificação simples) para confirmar a correcta implementação dos requisitos que especificaste para o sistema. Mapear cada caso de teste ao(s) respectivo(s) requisito(s).

Nota: Exemplo de especificação simples:

Testar que no momento de registo de um novo utilizador, o mesmo recebe um email para confirmar o seu registo em menos de 5 minutos. Caso o mesmo nunca receber o email o registo fica pendente. Caso o email chegue depois de 5 minutos, o registo não deve ser confirmado e um novo email deve ser gerado.

Nota: Um requisito pode perfeitamente ser não testável de forma dinâmica, nesse caso apresenta como o mesmo poderá ser verificado.

[EN]

Define a set of tests (in the form of a simple specification) to confirm the correct implementation of the requirements you specified for the system. Map each test case to the respective requirement(s).

Note: Simple specification example:

Test that when a new user registers, they receive an email to confirm their registration in less than 5 minutes. If the person never receives the email, registration remains pending. If the email arrives after 5 minutes, the registration must not be confirmed and a new email must be

TST-01: Testar a capacidade do sistema de garantir a integridade dos dados armazenados, processados e transmitidos, prevenindo alterações não autorizadas. Pode ser testado efetuando uma modificação e verificar se o sistema bloqueia a alteração não autorizada. O sistema deve prevenir a alteração e manter a integridade dos dados.

TST-02: Testar a capacidade do sistema de atribuir e gerir responsavelmente permissões e acessos, garantindo que cada utilizador tem apenas as autorizações necessárias. Pode ser testado atribuindo permissões específicas e verificar se o sistema as aplica corretamente. O utilizador deve ter acesso apenas às funcionalidades autorizadas.

TST-03: Testar a capacidade do sistema de garantir a confidencialidade das informações sensíveis, assegurando que apenas utilizadores autorizados têm acesso a dados sensíveis. Pode ser testado tentando efetuar o acesso a dados confidenciais sem as devidas permissões. O sistema deve negar o acesso não autorizado.

TST-04: Testar a capacidade do sistema de garantir a disponibilidade contínua dos serviços críticos. Pode ser testado gerando uma sobrecarga simulada e verificar como o sistema responde. O sistema deve manter a disponibilidade e responder de maneira adequada.

TST-05: Testar a capacidade do sistema de manter registos detalhados de atividades relevantes, permitindo a deteção de comportamentos anómalos ou tentativas de violação. Pode ser testado realizando uma tentativa de violação e verificar se o sistema regista a atividade. O sistema deve registar a tentativa de violação para posterior auditoria.

TST-06: Testar os procedimentos de resposta a incidentes do sistema. Pode ser testado simulando um incidente de segurança e verificar como o sistema responde. O sistema deve identificar, analisar e mitigar rapidamente o incidente, com comunicação transparente às partes interessadas.

Comentário:
TST-01: Devem ser testadas as alterações tipo diferentes, não apenas uma

TST-02: Testar todos os tipos de utilizadores e de permissões

TST-04: O que é responder de maneira adequada? Deve ser definido dependendo do teste e do caso de "falha"

TST-05: Todos os tipos de violações ou comportamentos anómalos possíveis devem ser testados

TAT-06: O sistema terá essa capacidade?

Pergunta **6**

Respondida

Nota: 3,00 em 3,00

[PT]

Para testar a robustez da solução, foi planeado efectuar alguns testes de Fuzzing e contratar um especialista para executar Penetration Testing ao sistema, nesse sentido:

a) Lista duas vantagens em fazer Fuzzy testing no contexto da solução. (podes identificar dois exemplos do que poderia ser encontrado com Fuzzy testing)

b) Identifica e descreve brevemente (até 100 palavras cada) dois ataques de segurança que poderiam ser descobertos ao aplicar a metodologia de penetration testing. (Podes identificar a vulnerabilidade e o interface relacionado por onde o PenTester pode explorar a vulnerabilidade)

[EN]

To test the robustness of the solution, it was planned to carry out some Fuzzing tests and hire a specialist to perform Penetration Testing on the system, in this sense:

a) List two advantages of doing Fuzzy testing in the context of the solution. (you can identify two examples of what could be found with Fuzzy testing)

b) Identify and briefly describe (up to 100 words each) two security attacks that could be discovered when applying the penetration testing methodology. (You can identify the vulnerability and the related interface through which PenTester can exploit the vulnerability)

a) Fazer Fuzzy testing no contexto da solução tem as seguintes vantagens:

- Gera automaticamente casos de teste, facilitando a deteção dos mesmos; A introduzir entradas inesperadas, como formatos de dados

- CSRF (Cross-site request forgery): Pode ser feito enganando um utilizador legítimo para executar ações não desejadas. Isto poderia incluir a manipulação de configurações de Smart Meters, ou a realização de ações críticas sem a devida autorização.
- SQLi (SQL injection): Pode ser feito injetando comandos SQL maliciosos. Isto poderia comprometer a integridade dos dados, permitindo ao atacante acessar ou manipular informações sensíveis dos Smart Meters.

Comentário:

Pergunta **7**

Respondida

Nota: 2,00 em 2,00

[PT]

Apresenta dois exemplos de procedimentos que deveriam fazer parte de um manual de instalação ou de utilização do sistema (nota que pode haver vários tipos de utilizadores: administrador, utilizador x, utilizador y, apenas consulta, etc.) para garantir que o sistema é utilizado/operado de forma segura e robusta.

Nota: Procedimentos, regras, policies, restrições, etc. devem existir em todos os sistemas e podem inclusivé estar especificados nos requisitos.

[EN]

Present two examples of procedures that should be part of a system installation or user manual (note that there may be several types of users: administrator, user x, user y, consultation only, etc.) to ensure that the system is used /operated safely and robustly.

Note: Procedures, rules, policies, restrictions, etc. they must exist in all systems and may even be specified in the requirements.

Os seguintes procedimentos deveriam fazer parte do manual de utilização do sistema:

1. Reinicio de um serviço (p/ novo cliente ou correção de problemas): Este procedimento destina-se a utilizadores com permissões de administrador ou técnicos autorizados e visa garantir o reinício seguro de um serviço associado a um Smart Meter. É de notar que esta operação é irreversível, pois os mesmo dados são perdidos para sempre.
2. Envio e troca de mensagem no portal: Este procedimento destina-se a utilizadores autorizados para garantir a comunicação eficaz através do portal SecureSmartMeter. Pode ser utilizado para enviar mensagens informativas, alertas ou para realizar trocas de informações relevantes. O envio de anexos é bastante limitado, podendo apenas enviar anexos até 5mb e num conjunto de formatos que se encontram conforme as políticas de segurança. Por motivos de segurança e confidencialidade, o email utilizado neste portal

Comentário:

Pergunta **8**

Respondida

Sem avaliação

[PT] Introduz o teu número de aluno:

[EN] Introduce your student number:

118345

Comentário:
OK

Obter a Aplicação móvel