Descriptif mission Schneideir à Grenoble, mission en anglais

In 2017, OWASP published TOP 10 risks for website security:

1. Injection: principle SQL
2. Broken authentification and Session Management
3. XSS: Cross-site scripting
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive data exposure
7. Missing fonction level access control
8. CSRF: Cross-site request forgery
9. Using components with known vulnerabilities
10. Unvalidated redirects and forwards

The Digital Risk within Digital Customer Experience require the improvement of our web security level and our security posture. Several projects on going to assess and remediate to all potential issues spread on different locations (on premise / Cloud). We need to improve our processes on software patch management, on our certificate lifecycle and the WebSites maintenance.

Tasks:

1. Enhance website security by digging its vulnerabilities via pentest tools, OWASP Zap & Burp Suite
2. Solve potentially unpredicted incidents and class its risks

Définition de la prestation
For that purpose we are looking for a security expert to :
1. Work with the different WebSite owners to fix web issues identified
2. Work on Security Incident and review the playbook
3. Work on PCI DSS Gap Remediation on Ecommerce Websites
4. Work on the required security training to developers or Admin

High expertise in Networking
PCI DSS knowledge: Governance (to put in place)
PCI DSS : Payment card industry Data Security Standard for the data security of credit cards

GDPR experience: reinforce our GDPR team, secure the data flow
GDPR: General data protection regulation

International Context
Fluent in English
Previous certified Auditor
Security standard: ISO7001, NIST, Certification as a Certified Information Security Systems Security Professional (CISSP), Certified Chief Information Security Officer (CCISO), or Certified Information Security Manager (CISM); Demonstrated experience managing threat response

Cybersecurity Standards:
NIST: (National institute of standards and technology) CSF (Cybersecurity Framework)
Identify – Protect – Detect – Respond – Recover
ISO/IEC 27001 and 27002: International Organisation of standardization/ International Electrotechnical Commission

Cybersecurity Certifications:
CISSP: (ISC) (Certified Information Systems Security Professional)
C|CISO: (EC-Council)(Certified Chief Information Security Officer)
CISM: (ISACA) (Certified Information Security Manager)
C|EH: (EC-Council) (Certified Ethical Hacker)
C|ND: (EC-Council) (Certified Network Defender)
C|HFI: (EC-Council) (Computer Hacking Forensics Investigator)

Ability to present problems in the larger scope of Business strategies
·Excellent written and verbal interpersonal skills
·Customer service-oriented mindset
·Ability to organize and facilitate meetings and workshops
·Ability to conform to shifting priorities, demands and timelines through analytical and problem-solving capabilities
·Experience & understanding of the complexity of working in a global project team
·Ability to identify issues/risk, analyse and understand underlying causes and devise appropriate action plans
·Ability to work with maximum autonomy
Livrables
Study of a managed SSL certificate platform management
SSL: Secure Socket Layer / Transport Layer Security/Application Layer
Deprecated in 2015 by TLS
TLS comprises two layers : TLS records and TLS handshake protocols

GDPR: reinforced
PCI DSS Governance put in place
Autres
Plan Projet, Principaux jalons
Q3 Q4
Autres informations
Environnement technique
Environnement technique
Domaines techniques
Administration réseau
Sécurité
Technologie Web
Environnements linguistique
Anglais

EBIOS: Expression des besoins et identification des objectifs de sécurité

- Étude de contexte
- Étude des besoins de sécurité
- Étude des menaces
- Identification des objectifs de sécurité
- Détermination des exigences de sécurité

F5 Networks:

- Nginx

LTM: Local Traffic Manager

APM: Access Policy Manager

PALO ALTO Networks:

- Technologie: Stateful Inspection – Pare-feu
- Technologie: Intrusion Prevention Système

MEHARI : Méthode harmonisée d’analyse des risques

Splunk : for Cybersécurité

- Splunk Enterprise Security – SIEM solution
- Splunk Phantom
- Splunk User Behavior Analytics
- Splunk Insights for Ransomware

Ansible : Configuration Management Software