

Onur AYYILDIZ

Information Security & Risk Manager

(Istanbul | Turkey) (onur.ayyildiz@gmail.com) (+905343428639)

PROFESSIONAL SUMMARY

Highly accomplished Security Team Manager with 15+ years of experience in cyber security. Having a sound knowledge information security, IT Risk and Governance and highly experienced in penetration testing, vulnerability management, incident response, application security and secure software development lifecycle (SDLC). Over the years, gained incomparable critical thinking and analytic detail-oriented skills, ability to deliver superior results under extreme pressure, unflinching flexibility, and adaptability to constantly changing circumstances. Adept at designing, building, implementing, managing, supporting, and enhancing key technologies and solutions.

Holding industry recognized certifications; (CISSP) - (C|CISO) - (CEH) – (PCI-DSS)

Technology Stack: COBIT, NIST, GDPR, CIS, PCI-DSS, ISO27001, SIEM(Qradar), Firewall, IPS/IDS, WAF, EDR/EPP, Anti-Virus/Malware/Spam, DLP, URL-Filtering, VPN, penetration testing, vulnerability assessment

Key areas of expertise:

- Cyber Security
- Information Security
- IT Risk Management
- IT Governance
- Penetration Test
- Vulnerability Assessment
- Security Operation Center
- IT Budget Management
- Incident Response
- Application Security

PROFESSIONAL EXPERIENCES

Information Security Manager, Anadolu Sigorta, Istanbul, TR, 2020-Present

Founded in 1925, as a privately-owned insurance company, Anadolu Insurance Company has played an important role in the development of the insurance industry in Turkey. It serves more than 10 million customers with more than 2500 business partner and more than 2000 employees.

- Collaborating with business and technical teams to create, manage, and initiate Cyber Security and Information security strategy to become a part of the culture for the company.
- Executing the management of the first/second line of defence and offense teams with the help of 15+ cyber security engineers to secure 200+ application and 1500+ servers with 4PetaByte data.
- Ensuring Cyber Security Operation Center monitors and responding to cyber-attacks 24/7, developing use-cases and playbooks, and conducting vulnerability scans and penetration tests to combat cyber-attacks.
- Serve as a key member of the company's Information Security Compliance Program by supporting ongoing compliance activities and monitoring efforts across different Regulations and GRC Standards (PCI, ISO, GDPR, COBIT others) as applicable and succeeded in being the first insurance company to get PCI DSS compliance certification in Turkey.
- Consults with information security risk engineers to analyse it environment of vendors providing various IT services to company.
- Managing Security operation team which are responsible for;
 - Configuring, troubleshooting and administration of Firewalls, IPS, Anti-Virus, URL Filtering systems.
 - Administration of MPLS, internet, local networks, Load Balancer and VOIP systems

Assistant Manager, Anadolu Sigorta, Istanbul, TR, 2018 – 2020

- Managed the Security Engineering team that develops 495 use cases and manages SIEM (Security Information Event Management).
- Reported security activity and threat reports to senior management.
- Guided and mentored all the managers in company and all the team members in IT Departments in all aspects of Cyber Security.
- Identified vulnerabilities as well as created and executed solutions
-

Information Security Architect, Anadolu Sigorta, Istanbul, TR, 2009 – 2018

- Designed, reviewed and approved of information security architecture, developed IT Security strategy which incorporated Anadolu Sigorta's business goals.
- Conducted penetration tests to identify vulnerabilities and weaknesses of IT systems and projects.
- Managed Log management systems. (Qradar)

- Performed and managed penetration tests, vulnerability management and security incident detection processes.
- Managed security audits performed by third parties.
- Managed network security systems such as Firewalls, IPS/IDS Solutions, Anti-Spam/Anti-Malware, and web URL proxy systems.
- Managed VPN and Load Balancing and WAF Systems (Citrix NetScaler and F5)

Network and Security Administrator, Mavi, Istanbul, TR, 2004 – 2009

- Managed all network and security infrastructure components.

EDUCATION

- Executive Development Program, Koc University, Istanbul, TR
- Mathematics Engineering (Bachelor's Degree), YTU, Istanbul, TR

CERTIFICATES

- CISSP (Certified Information Systems Security Professional), ISC2 - *Credential ID 844209*
- C|CISO (Certified Chief Information Security Officer), EC-Council - *Credential ID ECC3748561920*
- CEH (Certified Ethical Hacker), EC-Council - *Credential ID ECC963249*
- PCI ISA (Internal Security Assessor), PCI - *Credential ID 802-289*
- IELTS (International English Language Testing) - *Score 6.5*

PROJECTS

1. Cybercop - SaaS Platform for Cybersecurity Rating Software (Spinoff) – 2022

- I am the owner of the idea. Collaborated with senior management and budget was taken, created a team, managed project from end to end.
- What Cybercop do;
 - Solving the risk analysis needs of insurance companies and determine the cyber risks of companies' digital inventories open to the outside world.
 - Monitoring the security performance of third and fourth parties as well as their own security performance.
 - Companies can regularly assess cyber risks in their Digital ecosystems.

2. Performing Internal/External Audits – (2012-2023)

- Audit, control, and review more than 50 audits and become the first PCI DSS certificated insurance company in Turkey.
- Prepared more than 100 document based on regulations and GRC Standards.

3. Information Security Awareness Education – (2012-2023)

- Planned and developed an enterprise-wide information security awareness program more than to 5000 users

4. Setting Up Security Operation Center – 2021

- Collaborated with a 8 member team that developed a new security operation center, monitoring the system which has 10.000EPS.

5. Setting Up Disaster Recovery Center – 2020

- Evaluate new DRC environment, updated to ISO22301 framework, and assume responsibility for client BCDR program.
- Plan and manage IT Disaster Recovery setup Project, had several DRC tests including interruption – simulation – tabletop exercises and reports to senior management.

SKILLS

- **Information Security Management** (*Vuln. Management, Penetration Testing, Information and Cyber Security Strategy, Treat Intelligence, Awareness*)
- **Network Security Management** (*Firewall, IPS/IDS, Waf, Anti-Virus and Malware, EDR*)
- **IT Risk and Governance** (*Cobit, Pci-Dss, ISO27001, GDPR*)
- **Personnel** (*Team Working, Problem Solving, Result Oriented, Work Under Pressure, Leadership Skills, Teaching and Training*)

LANGUAGES

English : Advanced