KEREM GOKTAY

Senior CyberSecurity Administrator

BASIC INFORMATION

Bakirkoy, Istanbul, Turkey
kerem@goktay.net, +905552379265
Website: goktay.net

JOB OBJECTIVE

As a seasoned Senior CyberSecurity Engineer with a proven track record in the industry, expertise in safeguarding digital assets and ensuring the resilience of complex systems. Specializing in the implementation of robust security measures, I have successfully navigated the evolving threat landscape, adapting strategies to mitigate risks and fortify organizational defenses.

My comprehensive experience spans the deployment and management of security solutions across diverse platforms, including Windows and Linux environments. Proficient in designing and enforcing security policies, security at the physical and virtual layer, management of security products, patch management, web security strategies and security automations (Security Scanning Automations Sast - Dast - SCA).

With a proven ability to collaborate seamlessly with cross-functional teams, I am adept at translating complex security concepts into business-oriented language. My goal is to bring a proactive and strategic approach to cyber security, ensuring the confidentiality, integrity, and availability of critical assets. As a Senior Cyber Security Engineer, I am poised to contribute my skills and leadership to elevate security postures and drive organizational success.

HIGHLIGHTS OF QUALIFICATIONS

Strategic Security Planning:

- Developed and implemented comprehensive cyber security strategies aligning with organizational goals and industry best practices.
- Conducted risk assessments and formulated mitigation plans to fortify infrastructure against emerging threats.

Incident Response Leadership:

- Led incident response teams in effectively mitigating and resolving security incidents, minimizing downtime and potential data breaches.
- Established incident response protocols, ensuring a rapid and coordinated response to security events.

Cross-Platform Expertise:

- Demonstrated proficiency in securing diverse environments, including Windows (2000, 2003, 2008, 2012, 2016,2019) and Linux (CentOS, Ubuntu), ensuring a holistic approach to cyber defense.

Scripting and Automation:

- Developed and implemented automated security processes using scripting languages such as Python and Bash, enhancing operational efficiency and reducing manual overhead.

Firewall Configuration and Optimization:

- Configured and optimized UTM firewalls, utilizing iptables and fail2ban to establish robust security measures and control network traffic effectively.

Load Balancing and Project Management:

- Successfully configured Load Balance systems, contributing to project success and the seamless provision of work services.
- Played a pivotal role in project management, ensuring timely and successful completion of initiatives.

Cloud Security Proficiency:

- Implemented and maintained secure cloud environments, with expertise in utilizing Microsoft Azure and Amazon AWS services.
- Executed projects involving virtualization, P2V, H2V, and V2H, showcasing adaptability to evolving technological landscapes.

Security Compliance and Auditing:

- Ensured compliance with industry regulations and standards, conducting regular security audits to identify and rectify vulnerabilities.

Continuous Professional Development:

- Kept abreast of the latest cyber security trends, technologies, and threats through continuous learning and attainment of relevant certifications.

Effective Communication:

- Collaborated seamlessly with cross-functional teams, translating complex security concepts into accessible language for non-technical stakeholders.

WORK EXPERIENCE

Senior CyberSecurity Administrator Oct 2021 - Present

TAV Technologies

Proactively monitored and maintained customer-facing system patches, reducing vulnerability exposure by X% through detailed risk analysis and prompt security updates. Identified and tested internet-sourced vulnerability codes, issuing alerts to teams and achieving a reduction in vulnerability response time by 50%, enhancing overall system security.

Conducting comprehensive website scans to detect vulnerabilities, coordinating with relevant teams for mitigation, and managing overall security within the XDR framework, including EDR, Mail, Vulnerability Management, and AV solutions. Overseeing continuous code security scans, guiding secure code writing practices, and conducting in-depth analyses of code-side vulnerabilities.

Taking proactive measures to safeguard the company's brand on the deep web, securing phishing domains, and eliminating fake marketplace applications.

Leading SOC teams, developing and implementing accurate rules for False Positives/Negatives, configuring DDoS systems to counter various attack types, and establishing and documenting security procedures for company-wide use.

Analyzing and configuring WAF systems to effectively address False Positive behaviors and enhance overall security posture. This encompasses a comprehensive and proactive approach to securing systems, codes, and online assets while effectively leading and collaborating with cross-functional security teams.

Being involved from the very beginning of the project to determine the security standard in new projects and playing an active role in the entire project

Senior Information Security Administrator Oct 2020 - Sep 2021

N11

Monitoring and updating the patch status of customer-serving systems, conducting thorough analyses of system vulnerabilities, and promptly addressing potential security risks. Proactively investigating and testing codes associated with vulnerabilities shared on the internet, issuing warnings to relevant teams, and overseeing the patching or closure process. Employing web scanning techniques to identify potential vulnerabilities on sites, collaborating with relevant teams to ensure swift mitigation.

Managing comprehensive security within the XDR framework, encompassing EDR, NDR, FIM, Mail, Vulnerability Management, and AV solutions. Implementing continuous code security scans, guiding secure code writing practices, and conducting thorough analyses of code-side vulnerabilities.

Taking proactive measures to secure the company's brand on the deep web, including the takeover of phishing domains and the removal of fake marketplace applications. Thoroughly checking vulnerabilities in container architecture and updating container images based on the latest vulnerability information.

Enhancing Splunk widgets, addons, dashboards, and reports to improve overall security monitoring and

reporting capabilities. Reporting situations subject to PCI Certification and implementing necessary

System Engineer Feb 2019 - Nov 2020

Dogus Media Group

• Upgrade Checkpoints.Remove VSX systems to Core system.
• All Hyper-V Infrastructure migrate to Vmware Infrastructure. Setup Dswitch - HA and DRS Systems.
• Upgrade Windows 2003-2008-2012 to 2016 and 2019 core systems.
• Migrate Ntv.com.tr .net to core project on Azure.
• Migrate Web Project AWS To Azure & Service conversion (Project name PuhuTV)
* Manage all servers and clients security patching
* Planning DevSecops Proccess

System Engineer Feb 2018 - Feb 2019

Hürriyet

Implemented a transition structure to a more secure 802.1x wireless system.
Established a distribution server to efficiently handle incoming data, creating image files for worldwide agencies.
Worked on DRC systems within the Amazon environment, addressing missing sites and ensuring seamless operation in a 7x24 mode at both Istanbul and Amazon locations.
Acquired proficiency in Active/Active mode and gained expertise in DevOPS systems, contributing to effective system learning and management.
Optimized MSSQL, IIS, and Varnish to eliminate overloads, resulting in improved system performance.
Rectified deficiencies in the existing antivirus structure, implementing a sandbox solution to identify unknown sources and enhancing security through the utilization of Log products and open-source Siemens products.
These initiatives collectively elevated the overall security posture while fostering efficient system operations and management.

IT Team Leader Feb 2015 - Feb 2018

Cardtek

Executed a seamless Active Directory migration involving domain transfer and successfully orchestrated the migration to Office 365, facilitating the smooth transfer of all mail data through a hybrid connection.
Configured Skype for Business to ensure all users could receive messages from external domains.
Transferred legacy SharePoint content (2003, 2010) to the modern Office 365 SharePoint platform.
Installed and configured Zenload Load Balancer, implemented DC Self password change for remote users, and set up monitoring tools PRTG and Observium for a comprehensive view of network components, including switches, firewalls, Windows Server, Linux Server, VMware, UPS, and Air Conditioning. Implemented VLAN separation structure for enhanced server and user management.
Achieved SSL Security levels from F to A, validated by Qualys Lab Check (https://support.cardtek.com). In response to potential disasters, established a Disaster Recovery Center (DRC) with a dedicated Data Center (DC) in Samsun, ensuring redundancy through private BGP. Implemented replication of structures in Amazon (AWS), Google Cloud, and Microsoft Azure environments outside of Turkey for DRC moments, synchronized at 15-minute intervals. Ensured correct backup procedures and redirected external users via DNS due to private BGP.
Evaluated and upgraded the existing antivirus structure to Nextgen, conducting comprehensive investigations on known solutions. After considering various products, including Cisco AMP, Comodo, Cynet 360, Kaspersky, McAfee, SentinelOne, Sophos, and TrendMicro, opted for Trend Micro - ATP for enhanced security measures.

System Administrator May 2013 - Feb 2015

Kariyer.net

• vCenter installation was performed. HA structure was established.
• Checkpoint which was working standalone in the system, was clustered with a second device.
• Websense was made obligatory and active to all of the company users.Users were restricted by proper

policies.
• Sync & Publish Software was activated for publishing operations for an already existed website.
• Information that passes through the firewall was interpreted by activating a syslog software Splunk
• Local side logs were collected by using a programme named “Logsign”. And local side logs were delivered to 5651 structure content.
• Problem in the “3cx VOIP Server” was solved by updating the server
• Maintanence and optimization of already existed Linux servers were performed. Excess use of source was minimized by dividing the task load between servers.
• Scattered images were reunited under a certain image server. Image servers were changed into CDN structure.

System Administrator Aug 2010 - Jun 2013
Info-line Rehberlik ve Cagri Merkezi
Conducted reconfiguration of existing servers to enhance efficiency and optimize performance.
Revamped and organized the phone operator and IVR structure for improved functionality.
Consolidated non-essential services and servers to streamline operations and resource utilization.
Orchestrated the integration of the entire intranet, centralizing it under a SharePoint platform.
Updated Exchange and ISA to the latest versions, ensuring compatibility and security enhancements.
Implemented a shift in the firewall structure to an aggressive mode, bolstering defenses against potential external attacks.

System & Engineer Jr Sep 2009 - Aug 2010
DOL
P2v transitions were made to bring all existing servers together.
A standard has been set for PC inventory collection.
The ticket system for the Client Representatives has been passed on.

System & Network Manager Feb 2008 - Jan 2009
Shnet Danismanlik
• Regular server and maintenance of affiliated companies, weekly / monthly onsite visit planning and team
• orientation
• Establishment / support of the accounting program named Nebim
• Weekly and Monthly reporting of new customers, testing of new programs in the company and customers,
• Decision steps and process of commissioning

System Administrator Feb 2007 - Jan 2008
Digitron Elektronik
Engaged as part of a consulting agency, undertook diverse responsibilities encompassing Active Directory Installation, Exchange setup, DHCP and DNS management, BES configuration, Network Topology design and implementation, Firewall system administration, Sound system integration, CCTV system deployment, Client Support, Market Research, Product Investigation, and Product Purchasing.
Served multiple companies, gaining extensive experience in nearly all facets of IT operations. The dynamic nature of this role exposed me to a wide spectrum of IT tasks, contributing to a comprehensive skill set and a thorough understanding of various company infrastructures.

System & Network Manager Jan 2005 - Jan 2007
Cetinel Sogutma Sistemleri
In the company, an active directory was established and employees were given simple technical computer training.
The solar system was selected and installed as an ERP program according to the requirements of the company. Required for system users
A small training was given to them.
Set up camera and security system to be monitored centrally and over the web

EDUCATION

CyberSecurity Aug 2024 - Jun 2025
Ahmet Yesevi University (Master Degree)

Management Information Systems Sep 2019 - May 2024
Anadolu University (Bachelor Of Science)

Computer And Information Engineering / Information Technology July 2018 - Feb 2020
Sakarya University (Master Degree)

Public Relations and Advertisement Promotion Sep 2012 - Aug 2016
Ataturk University (Bachelor Of Science)

CERTIFICATIONS

Microsoft Certified: Azure Solutions Architect Expert
Microsoft Certified: Cybersecurity Architect Expert
Microsoft Certified: Azure Security Engineer Associate
Google CyberSecurity
Fortigate Network Security Expert Certification NSE 2
Fortigate Network Security Expert Certification NSE 1
F5 Networks Local Traffic Manager(LTM)
F5 Networks Application Security Manager(ASM)
Microsoft Trainer
Microsoft 365 Certified: Administrator Expert
Microsoft 365 Certified: Teams Administrator Associate
Microsoft Certified: Identity and Access Administrator Associate
Microsoft Certified: Security, Compliance, and Identity Fundamentals
MCSE: Productivity Solutions Expert
MCSA: Windows Server 2016
MCSA: Windows Server 2012
Microsoft® Certified Solutions Associate: Windows Server 2008
Microsoft Certified Professional
Microsoft® Certified IT Professional: Enterprise Administrator on Windows Server 2008
Microsoft® Certified Technology Specialist: Windows Server 2008 Network Infrastructure, Configuration
Microsoft® Certified Technology Specialist: Windows Server 2008 Applications Infrastructure, Configuration
Microsoft® Certified Technology Specialist: Windows Server 2008 Active Directory, Configuration

INTERESTS

Following new technology blogs and websites
Travel to new cities
Join to nature tours

PERSONEL INFORMATION

Date of birth :
13.08.1987
Marital Status : Single
Military : No military Obligation
Driving License : B Class

D.I.S.C.

• Independent
• Introduce original, interesting ideas and alternative solutions
• Change-orianted. Open to new ideas.
• Competitive. Evaluat the opportunities
• Persuasive.Want to take responsibility for important jobs.
• Willing and proccess-oriented.
• Needs reward and motivation. Want to be appreciated.
• Want to be accepted of his business and the position by others
• Want to influence with his success.
• Not a rule based person. Use initiative and apply his own methods
• Self-centered.
• Optimistic

REFERENCES

Özgür Daldaban- CIO - Doğan Holding - +905497465816
Kevork Malhas - CEO - Digitron - +905325740898