Leo Golas, CISSP
E-mail: hiring@leogolas.com
Website: http://www.leogolas.com
Mobile: 516-939-8156

OBJECTIVE

I am seeking a challenging role as a cybersecurity manager/technical leader that combines people and technical leadership, strong hands-on implementation of enterprise security, technical architecture, software development with project execution and problem solving that will make an impact on the overall bottom line.

EDUCATION

- B. Tech in Information Technology: Applied Computer Programming from Briarcliffe College, 2007
- Certified Information Systems Security Professional (CISSP) License 420821

EXECUTIVE SUMMARY

- 12+ years of IT and Enterprise Security experience covering a large facet of various security domains like Access Control, Cryptography, Governance and Information Risk, Application Security, and Operations Security.
- Experience in architecting, implementing & supporting Identity Management, LDAP Directories, Provisioning/Identity Workflows, Access Management, Single Sign on (SSO), Role Based Access Control (RBAC) Auditing, Database design, Database Auditing, SPML, Java/JSP Programming, Web Services, Attestation, and Report Generation.
- Administration of UNIX and Windows systems, including installation, configuration, tuning, upgrading, deployment, configuration, management, backups and maintenance.
- Successfully lead large mission-critical projects, data center migrations, upgrade and consolidations, while maintaining business process continuity.

WORK EXPERIENCE

Manager (Cybersecurity/Advisory Services) — July 2017 – Present
Ernst & Young LLP, New York, NY

Project Description – Financial Services:

- Managed and led a group of engineers/developers in meeting milestones and in adhering to management's and the client's expectations.
- Setup and integrated ServiceNow, Esker and SAP as relying parties within ADFS. Developed custom ADFS Claim Rules for issuance authentication and authorization.
- Administrated, implemented, configured, backed up and secured AD, VMware, AWS, Azure, Office 365 (AAD/EXO), ADFS, FIM/MIM, CA SiteMinder, CA Directory, RSA SecurID, SolarWinds, PRTG and Windows Servers.
- Upgraded Forefront Identity Manager 2010 R2 (FIM) environment to Microsoft Identity Manager 2016 (MIM).
- Developed, updated and maintained various PowerShell and VBScripts.
- Developed and updated custom Forefront Identity Manager (FIM) C# rule extensions for each of the management agents/connectors based on new requirements gathered.
- Management of mailboxes, users, contacts and groups via Office 365 UI and PowerShell commandlets.

- Responsible for bringing up and securing several websites for the client on AWS and on Microsoft Azure.
- Launched and implemented several SSO initiatives leveraging CA SiteMinder (WAM) and ADFS (Federation).
- Managed and led a major project for Multi-Factor Authentication (MFA) using Duo Security's – Duo MFA.
- Decommissioned Windows Server 2008 R2 Domain Controllers and rolled out Windows Server 2012 R2 and 2016 RODCs.
- Provided oversight and security recommendations on linux based VMs (CentOS, Red Hat) located on AWS and Azure.
- Implemented enterprise security best practices according to NIST publications, CIS benchmarks (OS hardening) and ISO 27001 and 27002 standards.
- Implemented and maintained on-premise Microsoft PKI environment.
- Assisted in SOX Compliance reports on a quarterly basis.
- Involved in weekly infrastructure patching (patch Tuesday) using Windows Server Update Services (WSUS) and Shavlik/Ivanti, as well as vulnerability remediation (ex: Java and Adobe Flash/Reader) using Nexpose for vulnerability scanning of Datacenter resources.
- Leveraged and used TrendMicro (for Datacenter VMs), Symantec Endpoint Protection (for physical and Cloud) and Malwarebytes for Antivirus/Anti-Spyware/Anti-Malware scanning.
- Investigated the feasability and use of Microsoft's Intune MAM (Mobile Application Management) on top of existing MDM (Mobile Device Management) AirWatch software.
- Ran customized reports for management using a wide variety of different tools (ex: McAfee ESM/SIEM, Varonis DatAdvantage) and various scripts (ex: PowerShell).

Senior Associate (Cybersecurity/Advisory Services) July 2015 – July 2017
Ernst & Young LLP, New York, NY

Project Description – Financial Services:

- Responsible for administrating, implementing, configuring, backing up and securing AD, VMware, AWS, Azure, Office 365 (AAD/EXO), ADFS, FIM/MIM, CA SiteMinder, CA Directory, Hitachi Password Manager, RSA SecurID, SolarWinds, PRTG, Git and Windows Servers.
- Setup and integrated Office 365, Syncplicity, Cisco CUCM-IM and Cisco UC as relying parties within ADFS. Developed custom ADFS Claim Rules (ex: to block external traffic and only allow devices on the core network).
- Configured various Run Profiles and sequences for all of the FIM/MIM management agents.
- Developed PowerShell scripts and Task Scheduler tasks for automating and maintenance of the several servers and for archiving of log files.
- Developed and updated VBScript script for handling various tasks (for example: populating AD attributes).
- Developed and updated custom Forefront Identity Manager (FIM) C# rule extensions for each of the management agents/connectors based on requirements gathered.
- Management of mailboxes, users, contacts and groups via Office 365 UI and PowerShell commandlets.
- Responsible for bringing up and securing several websites for the client on AWS and on Microsoft Azure.
- Configured Site to Site (S2S) VPN with Fortigate and Azure.
- Leveraged the use of Puppet for configuration management on-prem and in the cloud (AWS).
- Handled User Migrations from one AD domain to another AD domain while maintaining and preserving the Office 365 mailbox and identity information.
- Performed a migration from Windows Server 2003 DCs and member servers to Windows Server 2012 R2. Migrated FSMO roles to new Windows 2012 R2 Servers.
- Provided oversight and recommendations on linux based VMs (CentOS, Red Hat) located on AWS and Azure.
- Integrated Hadoop (and Hadoop services) with Kerberos and AD for authentication.
- Implemented enterprise security best practices according to NIST publications, CIS benchmarks and ISO 27001 and 27002 standards.