|  |  |
| --- | --- |
| Name: | Doug O’Leary |
| Email: | dkoleary@olearycomputers.com |
| Phone: | 630-248-2749 |
| Summary: | Using my 30 years experience in IT and security, I specialize in architecting, automating, and securing processes and systems. |
| Employment: | * Multiplan Inc, UNIX manager/Cloud Security Eng, 9.5 years
* O’Leary Computers Inc, Consultant, 15 years
 |

Cloud architecture and security:

* Generated 1 and 3 year cloud security road maps with initial emphasis on generating a repeatable process for cloud asset inventory and on cloud governance.
* Drafted, coordinated, and implemented cloud security policies and cloud storage and encryption standards. Deconflicted new documents with existing policies and standards.
* Founding member of MPI’s Cloud Center of Excellence (CCOE) helping to generate the corporate cloud architecture emphasizing the pillars of the well architected framework.
* Defined requirements for cloud security posture management (CSPM) and SaaS security posture management (SSPM), worked with stakeholders to design POC tests, selection, and implementation.
* Participated in numerous application/process security reviews using STRIDE to ensure a complete and comprehensive review.

Team/personnel management:

* Reformed previously mismanaged group from open, internal conflict to highly effective, high performing and cohesive team.
* Managed systems starting with ~ 350 virtual and physical hosts, supported by 5-member team and ending with over 2,500 systems managed by 4 member team.
* Mentored/coached low performers to achieve their potential.
* Documented, drafted, and automated all standard processes and procedures.
* Documented, drafted, and executed all security procedures for hitrust, sox, and other security audits. Automated evidence collection reducing time from days to minutes.
* Supported diverse application teams including oracle dbas and middleware.

Company impact:

* Patching:
	+ Introduced the concept of routine, regular patching to MPI moving from paradigm of “don’t patch unless it’s broke” to quarterly patching process following standard SDLC cycle.
	+ UNIX team success prompted other teams (windows, dbas, middleware) to follow suit.
	+ Fully adopted/accepted patching process was a key component to hitrust certification on first attempt.

Company impact (cont):

* Configuration management (puppet)
	+ Took over mismanaged puppet enterprise roll-out that wasted $500,000 over 3 years with no ROI by implementing open source puppet in a week.
	+ Home grown/forge modules provided consistent, standard system configurations increasing system reliability and decreasing support ticket counts and outages.
	+ Standardized configurations and enforcement are another key contributing factor in hitrust certification and sox audits as well as the key force multiplier enabling us to increase system count 800% with reduced head count and lowest support ticket counts.
	+ Wrote external node classifier to use MySQL db as single source of truth making configuration decisions and modules significantly easier.
* Kubernetes (k8s)/rancher:
	+ Recognizing the security impact of standalone docker in production, I took over a slow moving k8s POC project creating 5 k8s operations ready clusters managed by rancher in 4 months.
	+ Developed, documented, and automated processes/procedures for k8s installation, upgrade, and patching.
	+ Facilitating k8s adoption and the advent of devsecops at MPI.
	+ Worked with appdev teams to implement multiple machine learning deployments and am working on a variety of POC projects.
	+ Converted clustered MySQL db to k8s based mariadb and deployed AWX in k8s to support IT goals and processes.

Automation:

* puppet external node classifier originally in perl, converted to python.
* ansible dynamic inventory script in python.
* ldap wrapper script originally in perl, converted to python, to handle ldap/ldif intricacies enabling people not sufficiently knowledgeable with ldap to maintain the directory.
* Modular bash scripts to handle audit data collection. Admin selects which audit type and functions to execute and the script collects data from in-scope systems, recording checksums to ensure data integrity. Results in a gzip file ready to be uploaded to auditors’ choice of tools. Reduces data collection days and sometimes weeks to less than an hour.
* Dozens of ansible playbooks to handle repeated tasks.

Miscellaneous:

* Current security certifications: CISSP, CISA, CCSK, and CCSP
* Current cloud certifications: Azure Admin/Solutions architect (expert), AWS Sysops Admin
* Expired certifications include RHCE (v5 and 6), OCP, HPUX, and Solaris.