Recent Selected Projects and Initiatives

K. M. Peterson, April 2024

Mail Server, DMARC/DKIM, account lifecycle management. Organization was losing access to and control over a local mail service, so implemented new business-specific service, using open-source tooling. Set up and established DMARC/DKIM infrastructure. Developed account lifecycle processes including connection to LDAP for authentication, certificate management and a process for mail forwarding for discontinued users.

To improve efficiency, auditing, and response, implemented Identity Management Domain (Red Hat **IdM**) providing back-end and login services for hosts, controlled access to services and email authentication.

Implemented **monitoring and alerting services using Elasticsearch (ELK)**. No solution in organization met security and availability requirements. In response, built centralized logging service with searches, dashboards, and process for PCI-compliant review and alerting, including integration of server logging, intrusion detection systems, and audit and firewall logs.

Organization previously using incomplete and generic security policy. Coordinated major upgrades to produce a **PCI-compliant security policy**, including development of classification criteria for data, organization-specific policy and compliance requirements, SOPs, and application and service-specific controls. Approximately 60% of original template content re-written. Several years of annual reviews/updates.

Nature of business not served by corporate outsourced **security training** - developed specific and PCI-focused presentation and materials relating to business and services, and harmonized PCI and corporate compliance requirements.

No single and appropriately-scaled solution available to meet Google Cloud inventory requirements, leading to develop applications to utilize GCP APIs to produce **inventory of all organization Cloud assets**, generate XLSX workbook as output (supporting compliance, cost management, and accounting requirements).

Working with feedback from PCI QSA, developed compliant **workflows in Jira** to improve processes for system changes, problem remediation, and user management.

In order to communicate unique and material nature of service, developed and maintained graphical descriptions **(diagrams) of networks (physical and VPC), servers, services** (Kubernetes and Cloud Instance-based), data flows, encryption, and voice processes. These were used for compliance purposes, education, and customer exhibits.

Because responsible for infrastructure and accountable for costs and compliance, developed applications to “wrap” application data for **encryption pipelines** for space management, accounting, and lifecycle processes. Included reporting on retention of sensitive data age and location.

As part of process of developing and maintaining security policy and processes, determined that without consistent agreements about threats and costs, directives lacked objective underpinning. Planned, implemented processes for and conducted **Risk Assessments** using *OCTAVE* methodology.

Faced with requirement for **File-integrity Monitoring (FIM)** on secure network, implemented solution that addressed actual risks by enumerating specific scenarios valid for environment and provided substantially greater assurance than provided recipe.

Service availability and quality were hampered by lack of visibility of internal metrics. Took on implementation of **monitoring data collectors** for Freeswitch, rtpengine, and other voice telephony services. Data collected for Zabbix, GCP Stackdriver, and ELK-based monitoring, reporting, and alerting.

Enabling end-users to also have visibility to internal state: using APIs, GCP PubSub, and Beats applications, ingested voice **telephony and application data for end-user dashboards**; conducted training and customization to provide access to non-technical users.

Working in organizations with unique characteristics such as research teams, often faced with requirements and challenges requiring agility. Managing network services at non-enterprise scale led to solutions such as implementation of **containerized applications for network and application management**: DNS, DHCP (ISC Kia), ELK, LetsEncrypt.

To maintain known state of servers/host software stacks, implemented local **mirrors** (with automatic updates and space management) of OS software and user applications (yum/dnf).

Automated build of Cloud Server instances using Packer, customized for GCP and AWS, automated configuration of voice telephony services including dialplans and network-specific setup.

Faced with need to balance security of private keys with configuration control requirements, **automated TLS certificate provisioning** and secrets storage in git repository using encryption.

Modernized "hand-built" application hosts supporting application by **automating server deployment** using PXE/Kickstart, Puppet. Implemented functionality including IPAM, server-specific certificate management (IdM), application stack installation and configuration, *auditd* setup and monitoring and SELinux across Dell and HPE hardware and virtual hosts (KVM).

Starting with no knowledge of Google Kubernetes Engine and other GCP technologies, worked as part of team to implement applications with **infrastructure deployment using Terraform, and application deployment using Ansible**. Successfully expanded scale and functionality over three-year period through migrations of physical servers in datacenters to Cloud while maintaining highly available, compliant, and actively-developed services.

In order to maintain high availability local engineering and research instances in sub-optimal office environment, developed **environmental monitoring** systems by researching available interfaces on local UPS and temperature monitors that were not otherwise being monitored. Set up data collection with applications to query and generate actionable alerting for team.

Focused on making team more efficient, fostered end-user **collaboration platforms** (Confluence, Nextcloud, local web servers). Developed significant amount of documentation on applications and processes including automated reporting of important configuration data. Implemented cloud-based backup of locally-stored data.

Having significant day-to-day responsibilities that required use of "root" passwords and understanding of risks of one person solely in possession of them, set up an **escrow process for critical secrets** data using "*n*-of-*m*" key recovery and ensured distribution of keys to management.

General Areas of Focus

Using open-source infrastructure when appropriate for scale of application services and supporting resources. Example: KVM rather than VMware.

Sharing knowledge: more eyes on a problem and more situational awareness from all users means more effective team. Examples: team-specific security training, accessible information on systems/services status.

Highly skilled and valuable teams are wasted when supporting infrastructure isn't a priority. Prioritizing uniformity of computational resources imposes friction that is proportionally costly when it affects high-performance workers. Being able to build small-scale services for networks with these kinds of requirements is essential. Examples: implementing local DHCP/DNS services (in containers) for local networks.

Understanding trade-offs in strategic when planning Cloud-based services: determining where the future scaling enabled by Cloud intersects with overhead, training, architecture, expected growth and other questions when starting up a project. When is "buy it" more costly than "build it"? Example: Nextcloud v. Microsoft Office?

Compliance/Infosec requirements are generally generic, and implementation without understanding the nature of the application environment might be considered "in compliance" but may be ineffective. Ultimately, effort expended solely to pass an assessment is actually wasteful if goal is to reduce actual risks. Example: Implementation of FIM.