ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Windows Domain Administration

At ISC, the goal of Systems Engineering is to ensure that your organization's computer system meets its intended functionality, performance, and reliability requirements while minimizing costs and risks. We apply engineering methods, strategies, and tools to integrate and make all components of a system operate together efficiently and effectively.
Our team of experts consider the entire system and its environment rather than concentrating on the individual components to achieve a holistic approach to problem solving. The focus is on examining, designing, creating, assessing, implementing, and maintaining the system during its lifecycle.

Among these are:

Windows Domain Administration
Manages a network of computers that run Windows server. This involves managing network service activities that require passwords, software restrictions and extra configurations to strengthen security and performance of an organization's network.

This includes:

- An **active directory** to organize assets on a network of computers. Recording users, computers, and network resources, plus giving administrators the ability to manage accounts and modify access privileges.

- **Group policy** is managed by an administrator who sets specific rules and restrictions for computers and users to interact with the network. Implementation of these policies maintains consistent security, access control, settings, and configurations across the network.

- **Network services** that enable computers to communicate and share resources on a network. These are management activities that require passwords, software limitations, and additional settings to support security and performance. Examples include, DHCP (assigns IP addresses to computers on a network), DNS (translates domain names into IP addresses), and VPN (allows users to connect securely to a network over the internet, file sharing, email, and remote access). Network functionality and user collaboration are both dependent on these services.

ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Server Administration

Server Administration is integral to the operation of computer servers in an organization. The technical infrastructure of computer servers consists of the hardware, software, network components, and security protocols used to support server operations. As well as monitoring to ensure they are operating as configured and offering technical support to users.

Typical servers used:

- **Windows servers** is a product of Microsoft that provides a platform for running applications and managing data storage, user accounts, and network services in a Windows-based environment.
- **Linux servers** are an open-sourced specialized operating system similar to Windows server in function and purpose, but designed to be more customizable, flexible, and cost-effective.
- **Synology NAS servers** allow users to store, share and access data content, such as files, photos, and videos from multiple devices anywhere with an internet connection. A user-friendly interface, with high storage capacity, and advanced features such as information backup and media streaming.
- **VMware** provides virtualization software products for servers, desktops, and cloud environments. This allows multiple virtual machines to run on a single physical machine, enabling organizations to improve server efficiency and flexibility while reducing costs. VMware offers a selection of software products, including cloud management and automation solutions.
- **Nutanix** provides hyper-converged infrastructure (HCI) solutions that combine storage, computing power, and networking into an easy-to-manage system. This simplifies technology infrastructure by consolidating multiple components into one system, reducing costs, and improving performance.
- **Windows Hyper-V virtualization Hosts** are servers that allow multiple virtual machines (VM) to run on a single physical machine, while improving efficiency and reducing hardware costs. This can allow users to create, manage, and move VMs (virtual machines) between physical hosts with ease, depending on the organization's policies, procedures, and ability. Users can run multiple VMs without compromising performance due to Hyper-V's performance and scalability. It provides a cost-effective and flexible solution for running multiple operating systems and applications on a single physical machine.

ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Backup Administration

Backup Administration refers to creating copies of important data to prevent loss due to unexpected events, such as a system crash or cyber-attacks. System administrators determine what data needs backup, how often, and where this will be stored. These backups are regularly tested and monitored to safeguard critical data.

Typical software used:

- **Veeam** is software that provides backup, recovery, and data management solutions for virtual and physical technology environments. The primary product helps organizations protect computer data by making copies of important files and programs, allowing for easy recovery in case of data loss. Veeam offers additional products for data management and monitoring depending on the needs of an organization.

- **Synology Active Backup** is software that automatically creates backups of important data and applications to protect against data loss or system failure. This works with different devices and platforms and provides monitoring and management tools. This is useful for organizations that need to protect critical data.

ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Cloud Services, and Cloud Infrastructure

Cloud Services Administration - support, migrations, and integrations are services that help individuals and organizations use and manage cloud services. This includes monitoring, maintaining, and providing technical support for cloud infrastructure, moving, and migrating existing data and applications to the cloud, and connecting different cloud services to work together.

Cloud services or SaaS (software as a service) are resources or services provided over the internet used for online storage, email, and computing power. Anywhere an internet connection is available, these services can be accessed, eliminating the need for physical hardware or infrastructure. This provides a flexible and cost-effective way to access technology and services.

Typical services used:

- **Microsoft 365 and Google Workspace** are business applications that help organizations with productivity, and communication, with a focus on cloud-based services and collaboration. Microsoft 365 includes applications, Word, Excel, PowerPoint, Outlook, and Teams - a video conferencing tool. Google Workspace includes Google Docs, Sheets, Slides, Gmail, and videoconferencing tools.
- **Egnyte File Service** is a secure file service that allows individuals and organizations to store, access, and share files from anywhere. This provides a centralized platform for securely storing, sharing, and collaborating on files, with tools for file synchronization, backup, and version control. Egnyte is useful for organizations that need advanced security features and multiple sharing options.
- **Duo and Okta SSO/MFA** (Single Sign-On/Multifactor Authentication) are separate applications that add an extra layer of security and convenience to the login process by connecting to an existing login system. While both applications offer similar functionality, each has unique features and customization options, the choice of which application to use depends on the specific needs and requirements of the organization.
- **Cloud Infrastructure** manages technical systems and infrastructure of a cloud technology environment. This involves designing and configuring the cloud network, monitoring for potential issues, and providing user support.

Usual operations completed in a cloud computing environment incorporate running virtual machines, storing data in the cloud, databases, virtual desktops, development, and safely connecting to on-premises systems. An organization only pays for the services used, which are deployed and utilized on an as-needed basis. Providing a cost-effective solution that replaces the need to own and maintain computer equipment or costly data center infrastructure.

Typical cloud platforms used are Microsoft Azure and Amazon Web Services (AWS).

ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Penetration Testing

Penetration testing entails actively taking advantage of system weaknesses to demonstrate how an unauthorized individual could compromise its security.
The process of identifying vulnerabilities in a computer system, network, or application that can be exploited by an attacker is called penetration testing, also referred to as “pen testing” or “ethical hacking”. The goal is to identify weaknesses or gaps in an organization’s security position before being uncovered by hackers.
The testing involves mimicking cyberattacks to reveal vulnerabilities on a client’s systems. Feedback and recommendations are provided to correct or reduce these vulnerabilities to enhance an organization’s security defenses.

Options for testing:

Mobile App Pentests

Mobile app pentesting is the process of finding potential security flaws in iOS or Android apps that can be taken advantage of by hackers to cause damage to the app.

Cloud Pentest

With a cloud pentest, you can evaluate the security of your cloud architecture and identify vulnerabilities that attackers may use to their advantage. There are several platforms where this may occur, including AWS, Azure, GCP, M365, Digital Ocean, and others.

Internal Pentest

To evaluate the security of your company’s internal network, internal pentests are performed with the aid of a VPN and active directory.

Web Application Pentest

The aim of a web app pentest is to scrutinize the security of an app that is typically working behind an authentication mechanism, such as a login.

External Pentest

Companies use external pentests to evaluate the security of their public assets and prevent hackers from taking advantage of any vulnerabilities.

ISC INTEGRAL SYSTEMS CORP

www.integralsystemscorp.com

Systems Engineering

Vulnerabilty Scanning

Vulnerability scanning aims to assess and identify security gaps within a computer system, network, or application. The focus is on generating a comprehensive list of potential security threats, without exploiting those vulnerabilities. The testing combines automated tools with manual techniques to reveal flaws such as software bugs, poor configurations, and substandard security policies.

A detailed report is generated after testing is completed that categorizes the discovered vulnerabilities based on the level of severity, and typically provides recommendations for mitigating the risks they pose. This information can enable organizations to take proactive steps towards improving their cybersecurity measures and minimizing the probability of a successful attack. Vulnerability scanning is an indispensable preventive measure for organizations seeking to improve their security position. It identifies weaknesses and offers a roadmap to improve digital systems and is more resistant to potential threats.

With vulnerability scanning, an organization can achieve operational security, avoid false positives, save time, and manage costs by:

- Easily tracking and identifying assets
- Discovery of domains and sub-domains
- Oversee cloud settings
- Conveniently scan assets on-site

Difference between Vulnerability Scanning and Penetration Testing

Vulnerability scanning is aimed at identifying potential weaknesses without being too broad or invasive. The goal of penetration testing is to understand the real-world risks by exploiting weaknesses through a more targeted and intrusive approach. Vulnerability scanning is often used as a precursor to penetration testing, and the two are complementary.