Cloud Security

Introduction to Cloud Computing

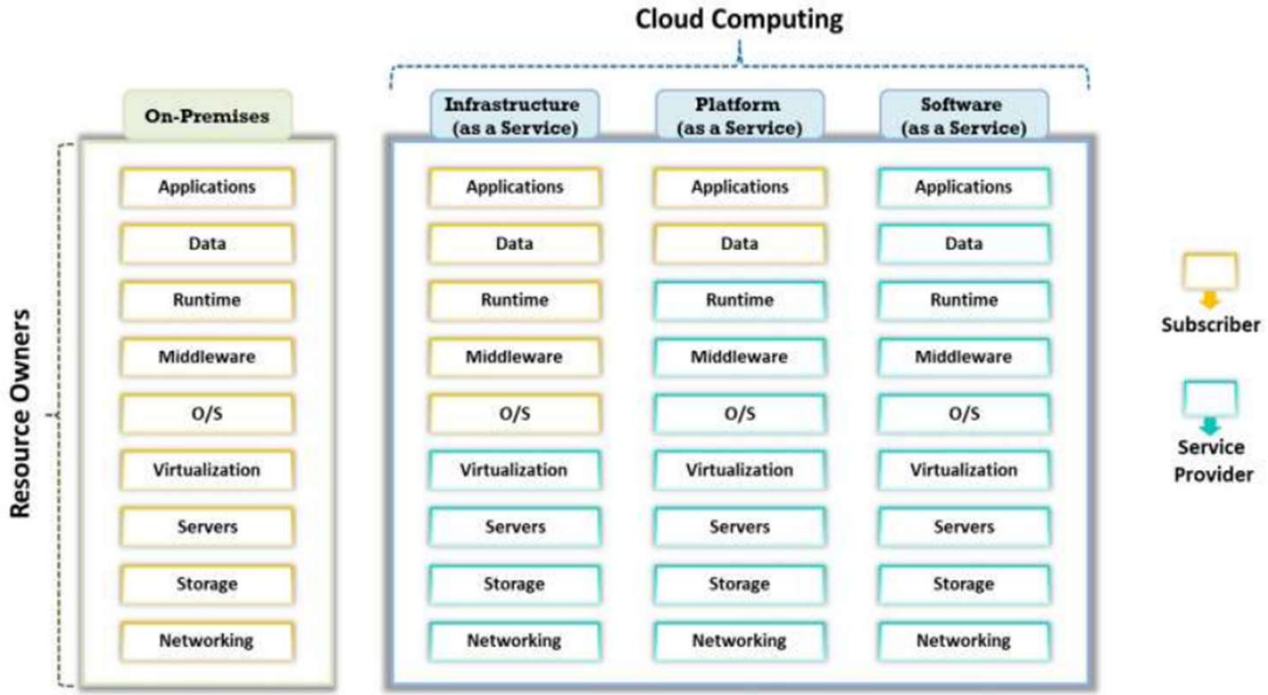
- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.
- Characteristics of Cloud Computing:
  - On-demand self-service
  - Distributed storage
  - Rapid elasticity
  - Automated management
  - Broad network access
  - Resources pooling
  - Measured service virtualization technology

Types of Cloud Computing Services

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (IaaS)
- Identity-as-a-Service (IDaaS)
- Security-as-a-Service (SECaaS)
- Container-as-a-Service (CaaS)
- Function-as-a-Service (FaaS)

Separation of Responsibilities in Cloud

(Shared Responsibility Model)



Cloud Deployment Models

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud
- Multi Cloud
- Distributed cloud

Cloud Computing Threats

1. Data breach/loss
2. Abuse and Nefarious Use of Cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Unsynchronized system clocks
8. Inadequate infrastructure design and planning
9. Conflicts between client hardening procedures and cloud environment
10. Loss of operational and security logs
11. Malicious insiders
12. Illegal access to cloud systems
13. Loss of business reputation due to co-tenant activities
14. Privilege escalation
15. Natural disasters
16. Hardware failure
17. Supply chain failure
18. Modifying network traffic
19. Isolation failure
20. Cloud provider acquisition
21. Management interface compromise
22. Network management failure
23. Authentication attacks
24. VM-level attacks
25. Lock-in
26. Licensing risks
27. Loss of governance
28. Loss of encryption keys
29. Risks from changes of Jurisdiction
30. Undertaking malicious probes or scans
31. Theft of computer equipment
32. Cloud service termination or failure
33. Subpoena and e-discovery
34. Improper data handling and disposal
35. Loss or modification of backup data
36. Compliance risks
37. Economic Denial of Sustainability (EDOS)
38. Lack of Security Architecture
39. Hijacking Accounts

CSP Native Service Nomenclature (The Multi-Cloud Rosetta Stone)

Why nomenclature matters.

- **The "Naming" Paradox:** In the cloud, names are often marketing-driven, not technical. For example, a "Bucket" (AWS) is a "Container" (Azure) which is a "Bucket" again (GCP).
- **Architectural Equivalence:** Most services across providers follow the same underlying distributed systems principles.
- **The Risk**: Miscommunication between teams, incorrect service selection, and slowed migration.
- **The Goal:** To enable "Cloud Fluency"—the ability to translate a business requirement into the specific native service of any provider without loss of meaning.
- Same services have different names across CSPs
  - Purpose: Avoid confusion during cloud operations
  - Storage: Amazon S3 vs Azure Blob vs GCP Cloud Storage
  - IAM: AWS IAM vs Azure Entra ID vs GCP IAM
  - Working: Services perform similar security functions

Storage Services (Storing unstructured data at scale)

Feature	AWS: Amazon S3	Azure: Blob Storage	GCP: Cloud Storage
Top-Level Unit	Bucket (Globally unique name)	Storage Account (Contains Containers)	Bucket (Globally unique name)
Data Unit	Object	Blob (Block, Append, Page)	Object
Key Advantage	Most mature; S3 API is the industry standard for 3rd parties.	Deeply integrated with Windows/AD; strong for "Data Lakes."	Best-in-class global consistency; very simple pricing tiers.

Virtual Compute & Modern Scaling

Provisioning raw power vs. managed platforms.

- **Virtual Machines (IaaS):**
  - **AWS (EC2):** Uses "Instance Types" (e.g., t3.medium). Highly customizable but can be complex to navigate.
  - **Azure (VMs):** Classified by "Series" (e.g., D-Series for general purpose). Very familiar to Windows Server admins.
  - **GCP (Compute Engine):** Unique "Custom Machine Types" allow you to pick exact CPU/RAM ratios rather than fixed sizes.

- **Serverless (FaaS):**
  - **AWS Lambda:** The pioneer. Best ecosystem for event triggers.
  - **Azure Functions:** Strongest for developers using C# or VS Code integration.
  - **GCP Cloud Functions:** Built on Knative; highly portable and simple to deploy.

Networking & Security Boundaries

How environments are isolated and connected.

- **Private Networks:**
  - **AWS VPC:** Region-specific. You must "peer" VPCs across regions.
  - **Azure VNet:** Region-specific, similar to AWS.
  - **GCP VPC: Global by design.** A single GCP VPC can span multiple continents, simplifying global architecture.

- **Identity (IAM):**
  - **AWS IAM:** Uses "Users," "Groups," and "Roles." Very granular.
  - **Azure Entra ID:** (Formerly Active Directory). Centralized identity for the whole enterprise (Office 365, etc.).
  - **GCP IAM:** Projects are the core unit. Policies are inherited from the "Organization" or "Folder" level.

Security Governance & Identity Structure

Understanding the hierarchy of control for Identity and Access Management (IAM) across providers.

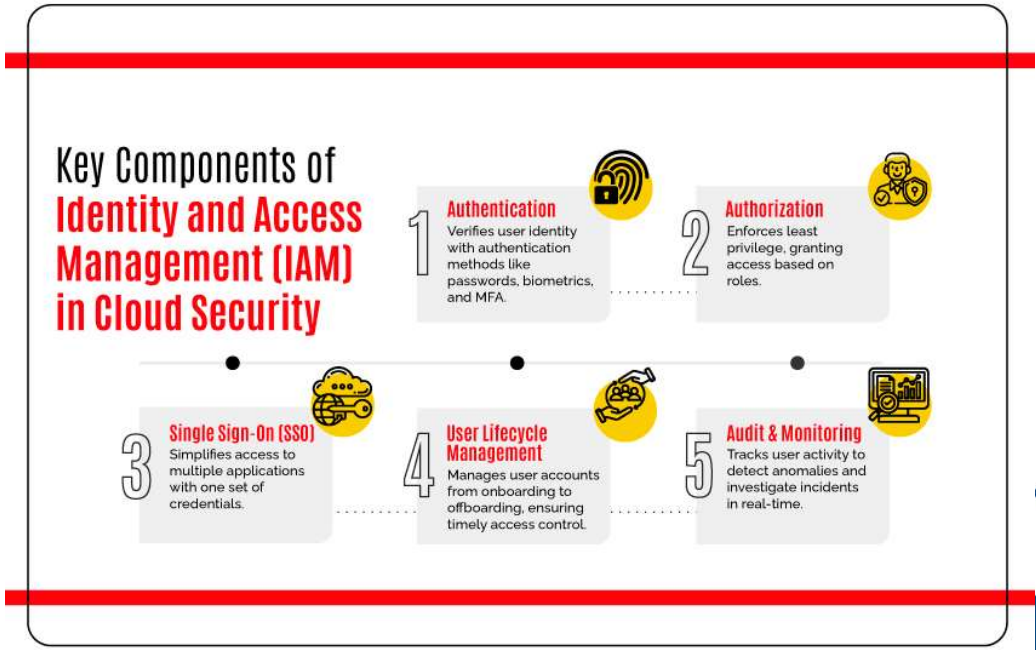
- **Comparison of Organizational Hierarchies:**
- **AWS**: Managed via AWS Organizations, utilizing Accounts as the primary boundary and Service Control Policies (SCPs) for top-down governance.
- **Azure**: Uses a Tenant as the top level, with management through Subscriptions and Resource Groups.
- **GCP**: Structured by Organization → Folders → Projects, where permissions are inherited downward.
- **OCI**: Uses Tenancy and Compartments to logically isolate resources for security and billing.

Identity and Access Management (IAM)

Controls authentication and authorization in cloud

- Purpose: Ensure least privilege access
- AWS: Account → IAM Users/Roles
- Azure: Tenant → Subscription → RBAC
- GCP: Organization → Project → IAM Roles

Policies define who can do what on which resource



Identity and Access Management (IAM)

A comparison of how each provider organizes its logical boundaries and management structures.

CSP	Top-Level Boundary	Secondary Level	Primary Unit for Resources
AWS	Organization	Organizational Unit (OU)	Account
Azure	Tenant (Entra ID)	Management Group	Subscription
GCP	Organization	Folder	Project
OCI	Tenancy	Parent Compartment	Compartment

Cloud Endpoint Protection & Vulnerability Management

Securing the "compute" layer from malware and known exploits.

- **Endpoint Detection & Response (EDR):**
- **Azure:** Features **Microsoft Defender for Endpoint**, providing advanced threat protection and post-breach detection.
- **AWS & GCP:** Often rely on specialized marketplace partners or native integrations with security agents.

- **Vulnerability Scanning:**
- **AWS:** Uses **Amazon Inspector**, which automatically discovers and scans EC2 instances and container images for software vulnerabilities.
- **Azure:** Integrated into **Microsoft Defender for Cloud**, providing continuous scanning of server workloads.

Cloud Security Posture Management (CSPM)

Identifying misconfigurations (like open S3 buckets) and ensuring compliance with industry standards (CIS, NIST).

- **Native CSPM Tools:**
- **AWS:** Uses **AWS Config** to track resource changes and evaluate them against "Config Rules" to detect non-compliance.
- **Azure:** Managed through **Microsoft Defender for Cloud**, which provides a "Secure Score" to quantify your current security posture.
- **Oracle (OCI):** Features **Oracle CloudGuard**, which monitors the tenancy for risky configurations and anomalous activities.

Cloud Logging – Unified Security Monitoring (SIEM/XDR)

Aggregating logs and alerts to respond to complex attacks.

The “Big Three" Solutions:

- **AWS: Amazon GuardDuty** (Threat Detection) and **AWS Security Hub** (Centralized dashboard for all security alerts).
- **Azure: Microsoft Sentinel**, a cloud-native SIEM that integrates directly with Defender for Cloud for rapid response.
- **GCP: Google Security Operations** (formerly Chronicle), designed for massive-scale log ingestion and sub-second searching.

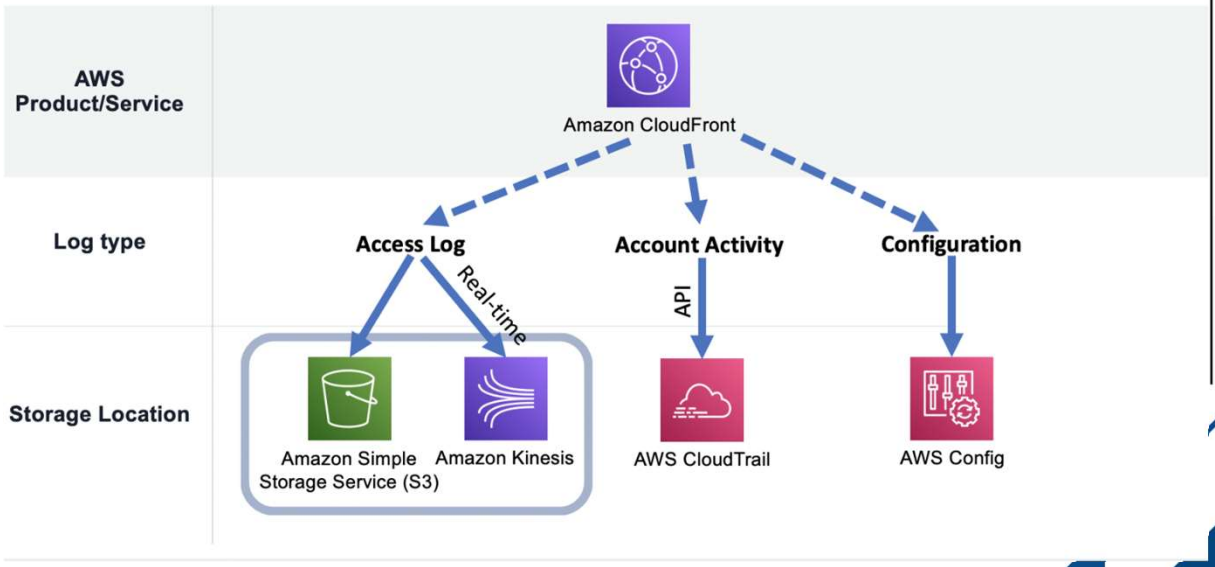
Log Types and Collection

Understanding what data is collected is essential for audit, forensics, and operational health.

- **Operating System Logs:** System-level events (e.g., startup, errors) recorded in Windows (Event Viewer) and Linux (/var/log).
- **Audit Logs:** Records of user actions, such as data access, configuration changes, and system setting modifications for compliance tracking.
- **Object Storage Access Logs:** Detailed logs tracking requests made to storage buckets (e.g., S3 Server Access Logs or Azure Blob Storage logging).
- **WAF Logs:** Logs from Web Application Firewalls that record incoming traffic patterns to detect and block malicious requests.

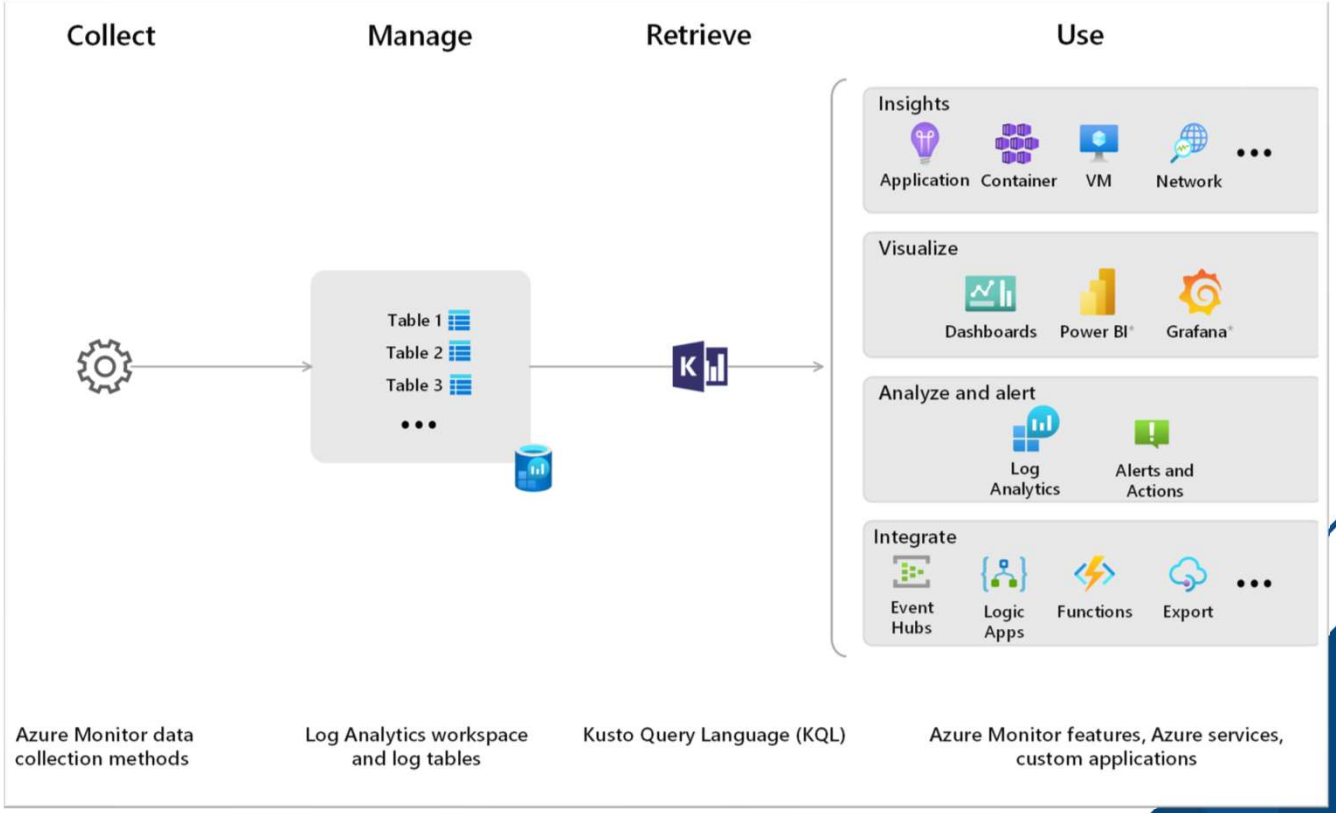
Log Aggregation – AWS

- CloudTrail records API activity
  - CloudWatch Logs collect system logs
  - Amazon S3 used for centralized storage
  - Working: Logs forwarded to SIEM for analysis



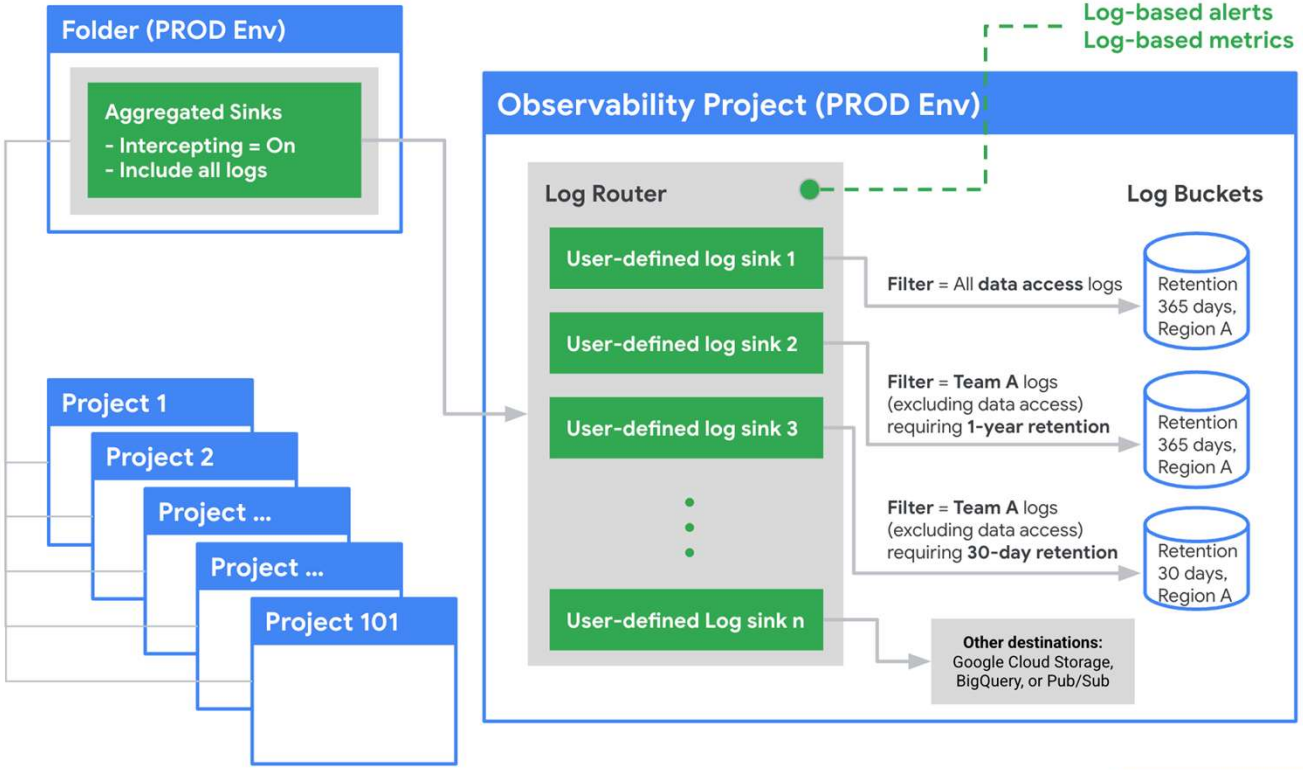
Log Aggregation – Azure

- Azure Monitor collects platform logs
  - Log Analytics Workspace stores logs
  - Event Hub streams logs to SIEM
  - Working: Integrated with Microsoft Sentinel



Log Aggregation – GCP

- Cloud Logging centralizes all logs
  - Supports VM, container, and service logs
  - Logs can be exported to SIEM
  - Working: Enables threat detection and investigations



Cloud Security Control Layers

1 Application	SDLC, Binary Analysis, Scanners, Web App Firewalls, Transactional Sec
2 Information	DLP, CMF, Database Activity Monitoring, Encryption
3 Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
4 Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
5 Trusted Computing	Hardware and software RoT and API's
6 Computation and Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
7 Physical	Physical Plant Security, CCTV, Guards

What is Cloud Hacking?

- Attackers exploit vulnerabilities existing in the cloud technologies to perform various targeted high-profile attacks on cloud storage systems, compromising the corporate and customers' data.
- The main objective of hacking the cloud environment is gaining access to user's data and blocking access to cloud services.

Is Cloud Computing Secure?

For most organizations, the journey to cloud is no longer a question of “if” but rather “when”, and a large number of enterprises have already travelled some way down this path.

Is cloud computing secure?

- A simple answer is: Yes, if you approach cloud in the right way, with the correct checks and balances to ensure all necessary security and risk management measures are covered.

Is Cloud Computing Secure?

- Companies ready to adopt cloud services are right to **place security at the top of their agendas**.
- the consequences of getting your cloud security strategy wrong could not be more serious.
- As many unwary businesses have found to their cost in recent high-profile cases, a single cloud-related security breach can result in an organization severely damaging its reputation – or, worse, the entire business being put at risk.

Is Cloud Computing Secure?

- *Those further along their cloud path are finding that, like all forms of information security, the question boils down to **effective risk management**.*

we outlined the different layers in the cloud services stack:

- **Infrastructure**-as-a-Service (IaaS)
- **Platform**-as-a-Service (PaaS)
- **Software**-as-a-Service (SaaS)
- **Business Process**-as-a-Service (BPaaS).
- These layers – and their associated standards, requirements and solutions – are all at different levels of maturity.

Is Cloud Computing Secure?

- The world of business is becoming more uncertain, as with new system architectures come new cyber threats. No longer can the mechanisms deployed in the past be relied on for protection”

  --Nick Gaines, Group IS Director, Volkswagen UK

- Different types of cloud have different security characteristics. The table in next page shows a simple comparison. (The number of stars indicates how suitable each type of cloud is for each area.)
- We choose to characterize these types as private, public and community clouds – or “hybrid” to refer to a combination of approaches.

Security Characteristics

Security characteristics of different types of cloud

	Private	Community	Public	Hybrid
Governance and enterprise risk management	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Data residency and jurisdiction	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Compliance and audit	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Access control	☆ ☆ ☆	☆ ☆	☆	☆
Shared resources and data segregation	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Security incident management	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Physical security	Dependent upon service	Dependent upon service	Dependent upon service	Dependent upon service
Privileged users	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Continuity services	Dependent upon business needs	Dependent upon business needs	Dependent upon business needs	Dependent upon business needs
Data disposal	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆

The ratings assume each item on the left is implemented appropriately.

Security Risks

- Organizations with defined controls for externally sourced services or access to IT risk-assessment capabilities should still apply these to aspects of cloud services where appropriate.
- But while many of the security risks of cloud overlap with those of outsourcing and offshoring, there are also differences that organizations need to understand and manage.

“When adopting cloud services, there are four key considerations:
1. Where is my data?
2. How does it integrate?
3. What is my exit strategy?
4. What are the new security issues?”
--Tony Mather, CIO, Clear Channel International

Security Risks

- **Processing sensitive or business-critical data** outside the enterprise introduces a level of risk because any outsourced service bypasses an organization's in-house security controls. With cloud, however, it is possible to establish compatible controls if the provider offers a dedicated service. An organisation should ascertain a provider’s position by asking for information about the control and supervision of privileged administrators.
- **Organizations using cloud services** remain responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subject to external audits and security certifications. Cloud providers may not be prepared to undergo the same level of scrutiny.
- **When an organisation uses a cloud service,** it may not know exactly where its data resides or have any ability to influence changes to the location of data.

Security Risks

- **Most providers store data in a shared environment.** Although this may be segregated from other customers' data while it's in that environment, it may be combined in backup and archive copies. This could especially be the case in multi-tenanted environments.
- **Companies should not assume service providers will be able to support electronic discovery,** or internal investigations of inappropriate or illegal activity. Cloud services are especially difficult to investigate because logs and data for multiple customers may be either co-located or spread across an ill-defined and changing set of hosts.
- **Organisations need to evaluate the long-term viability of any cloud provider.** They should consider the consequences to service should the provider fail or be acquired, since there will be far fewer readily identifiable assets that can easily be transferred in-house or to another provider.

Cloud Security Simplified

- As with all coherent security strategies, cloud security can seem dauntingly complex, involving many different aspects that touch all parts of an organization.
- CIOs and their teams need to plot effective management strategies as well as understand the implications for operations and technology.
- we outline the key considerations.
  - Management
  - Operation
  - Technology

Cloud Security Simplified

- **Management**
  1. Updated security policy
  2. Cloud security strategy
  3. Cloud security governance
  4. Cloud security processes
  5. Security roles & responsibilities
  6. Cloud security guidelines
  7. Cloud security assessment
  8. Service integration
  9. IT & procurement security requirements
  10. Cloud security management

Cloud Security Simplified

- **Operation**
  1. Awareness & training
  2. Incident management
  3. Configuration management
  4. Contingency planning
  5. Maintenance
  6. Media protection
  7. Environmental protection
  8. System integrity
  9. Information integrity
  10. Personnel security

Cloud Security Simplified

- **Technology**
  1. Access control
  2. System protection
  3. Identification
  4. Authentication
  5. Cloud security audits
  6. Identity & key management
  7. Physical security protection
  8. Backup, recovery & archive
  9. Core infrastructure protection
  10. Network protection


thank you

SKILL DEVELOPMENT INSTITUTE BHUBANESWAR | Managed by IndianOil

Aspire Mind Foundation

CYBERFRAT® AN ERM COMMUNITY

Windows & Linux Security

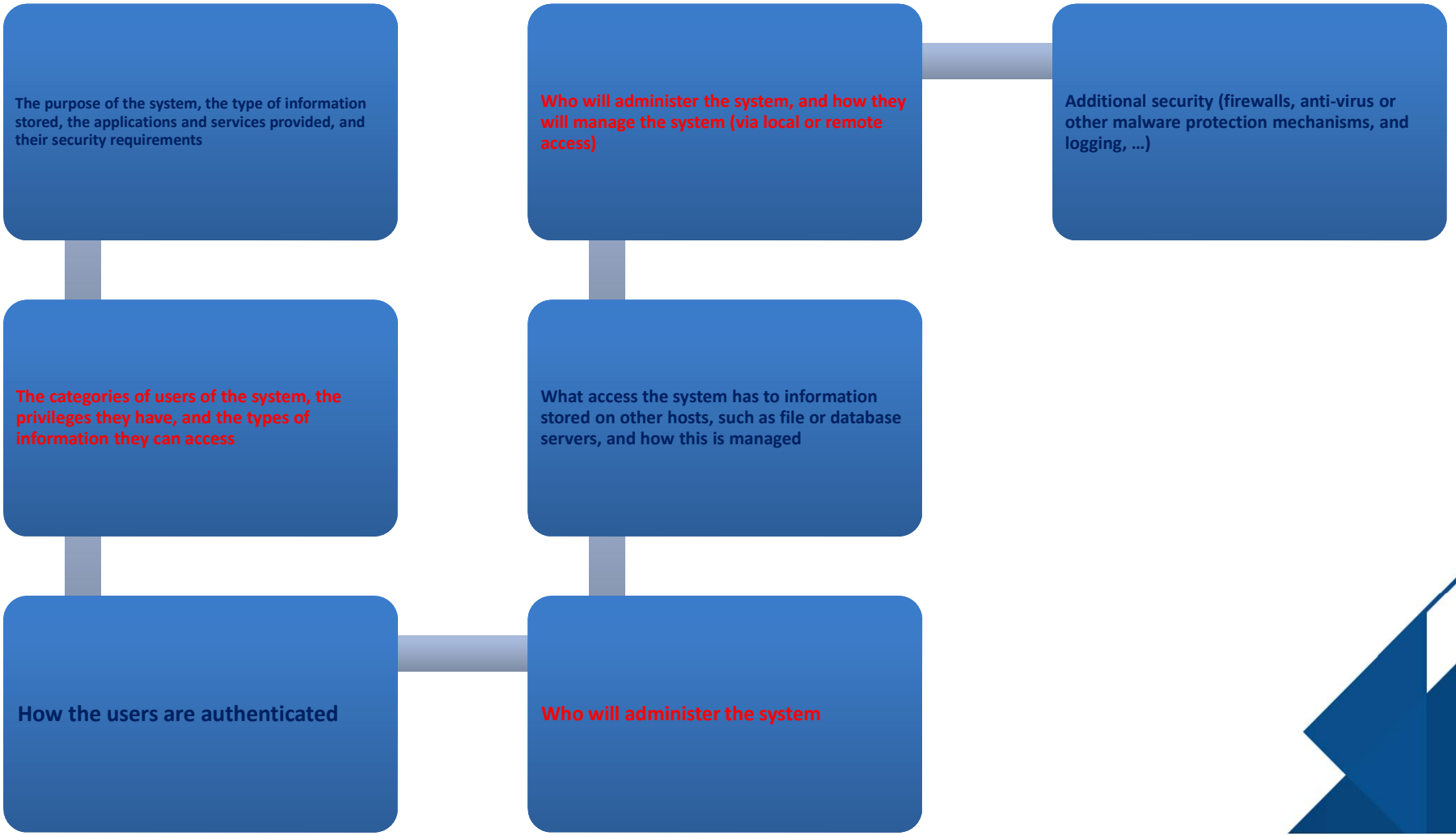
Operating System Security

- Possible for a system to be compromised during the installation process before it can install the latest patches
- Building and deploying a system should be a planned process designed to counter this threat
- Process must:
  - assess risks and plan the system deployment
  - secure the underlying operating system and then the key applications
  - ensure any critical content is secured
  - ensure appropriate network protection mechanisms are used
  - ensure appropriate processes are used to maintain security

System Security Planning

- The first step in deploying a new system is planning
  - Plan needs to identify appropriate personnel and training to install and manage the system
  - Planning process needs to determine security requirements for the system, applications, data, and users
- Aim: maximize security while minimizing costs

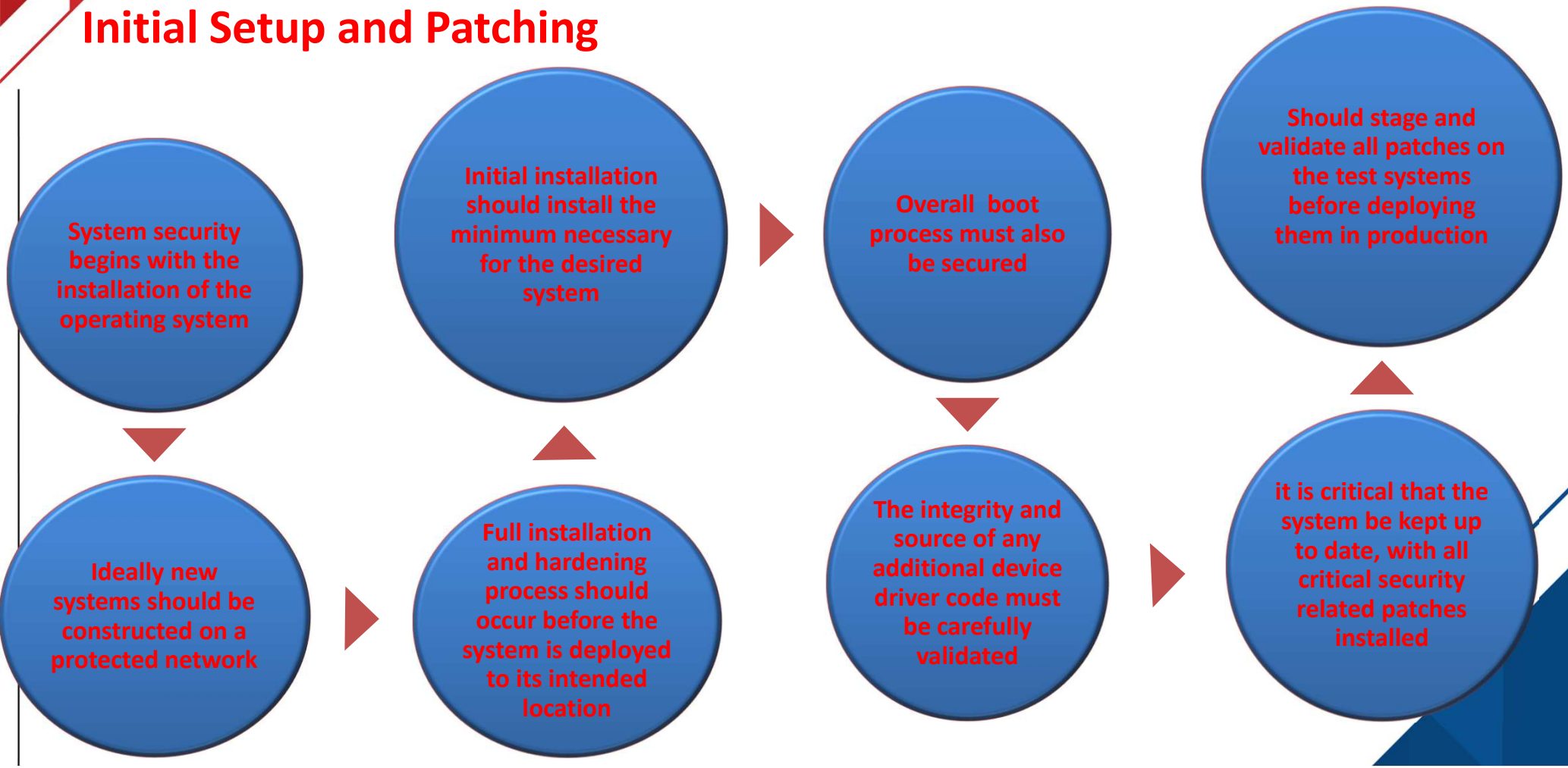
System Security Planning Process



Operating Systems Hardening

- First critical step in securing a system is to secure the base operating system
- Basic steps
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the identified security needs of the system
  - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
  - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

Initial Setup and Patching



Remove Unnecessary Services

- if fewer software packages are available to run the risk is reduced
- system planning process should identify what is actually required for a given system

- when performing the initial installation the supplied defaults should not be used
  - default configuration is set to maximize ease of use and functionality rather than security
  - if additional packages are needed later they can be installed when they are required

Configure Users and Privileges

- Not all users with access to a system will have the same access to all data and resources on that system
- Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

- System planning process should consider:
  - categories of users on the system
  - privileges they have
  - types of information they can access
- Default accounts included as part of the system installation should be secured
  - those that are not required should be either removed or disabled
  - policies that apply to authentication credentials configured

Configure Resource Controls

- Once the users and groups are defined, appropriate permissions can be set on data and resources
- Many of the security hardening guides provide lists of recommended changes to the default access configuration
- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing

System Testing

- Final step in the process of initially securing the base operating system is security testing
  - Goal: Ensure the previous security configuration steps are correctly implemented
- Checklists are included in security hardening guides
- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices

Application Configuration

- May include:
  - Creating and specifying appropriate data storage areas for application
  - Making appropriate changes to the application or service default configuration details
- Some applications or services may include:
  - Default data, scripts, user accounts
- Of particular concern with remotely accessed services such as Web and file transfer services
  - Risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server

Encryption Technology

A key enabling technology that may be used to secure data both in transit and when stored

Must be configured and appropriate cryptographic keys created, signed, and secured

If secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

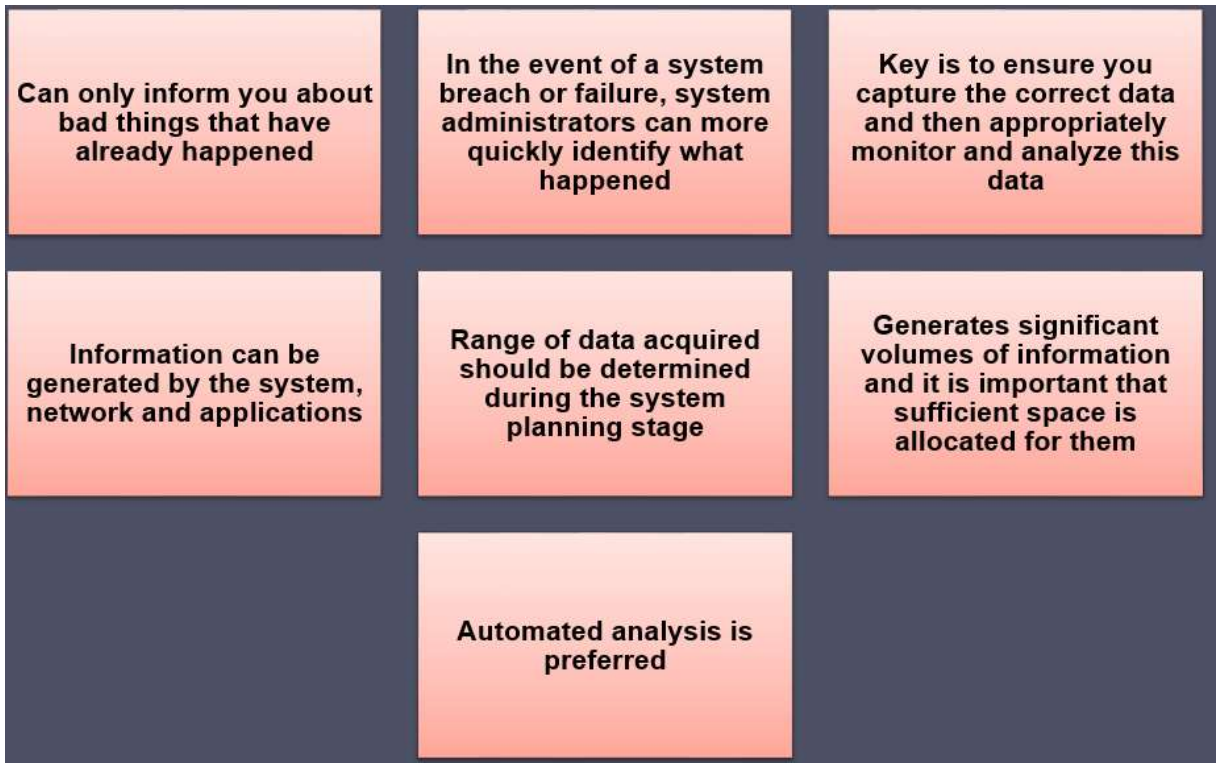
If secure network services are provided using SSH, appropriate server and client keys must be created

Cryptographic file systems are another use of encryption

Security Maintenance

- Process of maintaining security is continuous
- Security maintenance includes:
  - Monitoring and analyzing logging information
  - Performing regular backups
  - Recovering from security compromises
  - Regularly testing system security
  - Using appropriate software maintenance processes to patch and update all critical software, and to monitor and revise configuration as needed

Logging


Can only inform you about bad things that have already happened
In the event of a system breach or failure, system administrators can more quickly identify what happened
Key is to ensure you capture the correct data and then appropriately monitor and analyze this data
Information can be generated by the system, network and applications
Range of data acquired should be determined during the system planning stage
Generates significant volumes of information and it is important that sufficient space is allocated for them
Automated analysis is preferred

Data Backup and Archive

Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

Backup

Archive

The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

Needs and policy relating to backup and archive should be determined during the system planning stage

Kept online or offline

Stored locally or transported to a remote site

- Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

LINUX SECURITY

What is Linux ?

- Linux is a free open source operating system (OS) based on UNIX that was created in 1991 by Linus Torvalds. Users can modify and create variations of the source code, known as distributions, for computers and other devices. The most common use is as a server, but Linux is also used in desktop computers, smartphones, e-book readers and gaming consoles etc.
- It is also used by Hackers
- Linux Types :
  - Ubuntu
  - Redhat
  - Suse
  - Debian
  - Centos
  - Oracle

Hardening

- Hardening refers to providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as defense in depth. Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between. Each level requires a unique method of security.
- A hardened computer system is a more secure computer system.
- Hardening is also known as system hardening.
- Guides :
- Guides : CIS Benchmark
- Tools : Scap , Lynis

What if we don’t Hardening ?

Users and Groups

- Users and Groups are used to control access to files and resources . Different permissions are also applied depending on users and groups.

Users:

- Every user of the system is assigned a unique user id known as UID.
- Users names and UID'S are stored in this location -/etc/passwd. Users can't read ,write or executable each other's file without permissions.

Groups:

- Users are assigned to groups with unique group id numbers known as the gid.
- Each user is given their own group . gids are stored in this location -/etc/group.

File Security

File Permissions:

- Every file and directory in your UNIX/Linux system has following 3 permissions defined for all the 3 owners discussed above.
- Read (r): This permission give you the authority to open and read a file. Read permission on a directory gives you the ability to lists its content.
- Write (w): The write permission gives you the authority to modify the contents of a file. The write permission on a directory gives you the authority to add, remove and rename files stored in the directory. Consider a scenario where you have to write permission on file but do not have write permission on the directory where the file is stored. You will be able to modify the file contents. But you will not be able to rename, move or remove the file from the directory.

- Execute (x): In Windows, an executable program usually has an extension ".exe" and which you can easily run. In Unix/Linux, you cannot run a program unless the execute permission is set. If the execute permission is not set, you might still be able to see/modify the program code(provided read & write permissions are set), but not run it.

Special Permissions:

➢ In this we have four cases. They are :

1)SUID (Set – user Identification) for an execution.

2)SGID (set group ID) for an execution.

3)SGID (set group ID) for an Directory.

4)Sticky bit for a directory

LINK: https://thegeeksalive.com/linux-special-permissions/

INODES :

➢ An inode is a data structure on a traditional Unix-style file system such as UFS or ext3. An inode stores basic information about a regular file, directory, or other file system object.

➢ https://www.cyberciti.biz/tips/understanding-unixlinux-filesystem-inodes.html

Linux Server Hardening

Steps :

- Boot Security
- Patching Linux Kernel
- Remove Unused Software
- Strong Password Policy
- Securing Root Login
- Process Security

1.Boot Security :

- Boot loader is useful in preventing unauthorized users who have physical access to systems from booting using removable media like USB .
- LILO and GRUB are two boot security loaders for linux workstations.

GRUB	LILO
GRUB stands for Grand Unified Boot Loader	LILO stands for Linux Loader
It support for unlimited boot entries	LILO only support up to 16 different boot selection
GRUB boot from network	LILO does not boot from network
There is no need to change GRUB if configure file changed . GRUB is dynamically configure	There is need to change LILO if configure file changed . LILO is not dynamically configure
GRUB has interactive command interface	LILO does not have interactive command interface
GRUB has knowledge of file system	LILO does not have any knowledge of file system

➢LILO Configure File :

- ❖ Boot =/dev/had
- ❖ Map =/boot/map
- ❖ Install =/boot/boot.b
- ❖ Prompt
- ❖ Timeout = 100
- ❖ Compact
- ❖ Default = Linux
- ❖ Image = /boot/vmlinuz-2.4.18-14
- ❖ Label =Linux
- ❖ Root = /dev/hdb3
- ❖ Read-only
- ❖ Password=linux
- ❖ Other=/dev/had
- ❖ Label=windowsXP

- GRUB Configure File :

❖Default=0

❖Timeout=10

❖Splashimage=(hd1,2)/grub/splash.xp.gz

❖Password –md5 $1$0pevt0$y.br.18LYAasRsGdSKLY1p1

❖Title Red Hat Linux

❖Password –md5 $1$0pevt0$y.br.18LYAasRsGdSKLY1p1

❖Root (hd1,2)

❖Kernal /vmlinuz-2.4.18-14 ro root == LABEL =/initrd /initrd-2.4.18-14.img

❖Savedefault

❖boot

2.Patching Linux Kernel:

What is a patch?

- A patch is a small text document containing a delta of changes between two different versions of a source tree. Patches are created with the diff program.
- To correctly apply a patch you need to know what base it was generated from and what new version the patch will change the source tree into. These should both be present in the patch file metadata or be possible to deduce from the filename.

Patching Linux includes :

- Getting new kernel modules
- Editing LILO.conf
- Restarting LILO
- Write new MBR

Kpatch – Dynamic Kernel Patching :

- Kpatch is a feature of the linux kernel that allows live patching of a running kernel which allows kernel
- Patches to be applied to the kernel for security even through the kernel is still running

3.Remove Unused Software:

❑Commands:

- For Red Hat/ RHEL/ Fedora / Centos :

$ yum list installed

$ yum list packageName

$ yum remove PackageName

➢Debian/Ubuntu Linux :

$ dpkg –l

$ dpkg --info packageName

$ apt-get remove packageName

4.Strong Password Policy :

1) Configuration of shadow password:

❖Command:

Nano /etc/login.defs

❖Configuration Parameters:

PASS_MAX_DAYS=30

PASS_WARN_AGE=20

ENCRYPT_METHOD SHA512

LOGIN_RETRIES =5

2)Password Files in Linux:

/etc/Passwd	/etc/shadow
It has one way encrypted passwords are stored in a text file.	Shadow utils is a package in linux that's installed by default in most of the distributions.
This file is readable by any user in the system.	This directory is only accessible to root.

5.Process Security :

- It is a mix of administrative, engineering and behavioral activities focused on preventing undesired accidents and unexpected events that may have a negative impact to a given process.
- We have some components:
  - Exec thread
  - PID
  - Memory Context
  - Environment
  - Priority
  - Security Credentials
  - File descriptor

6.Securing Root Login:

- Disabling Root access via any console device (tty).
- edit the securetty file vim/etc/securetty and comment out the following lines:

tty1

#tty2

It means root is allowed to login at tty1. tty2 is disabled.

Operating System

- Patching and Software Updates: periodically patches are released for included software either due to security flaws or to include additional functionality.
- File System Configuration:
  - Create Separate Partition for /tmp: grep “[[:Space:]]/tmp[[:space:]]” /etc/fstab
  - Create Separate Partition for /var: grep “[[:Space:]]/var[[:space:]]” /etc/fstab
- Secure Boot Settings :
  - Set permissions on boot loader config: chmod og-rwx/boot/grub/grub.cfg
  - Set Boot Loader Password : grub-mkpasswd-pbkdf2
- Os Services:
  - Ensure rsh server is not enabled
  - Ensure telnet server is not enabled

SELinux

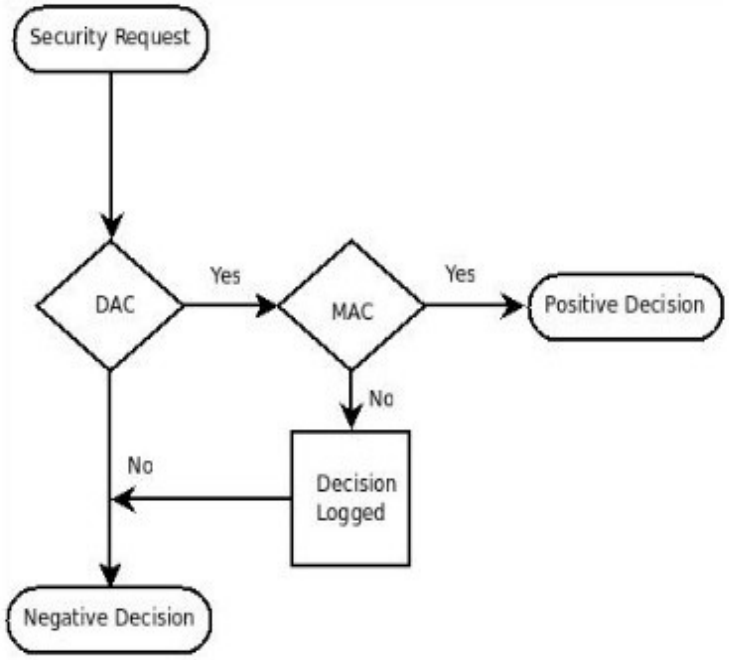
- Security-Enhanced Linux (SELinux) is a security architecture for Linux systems that allows administrators to have more control over who can access the system. It was originally developed by the United States National Security Agency (NSA) as a series of patches to the Linux kernel using Linux Security Modules (LSM). In SELinux has MAC and DAC

DAC	MAC
User has complete control overall programs it owns and execute.	Administrators manages the access controls unlike the users in DAC
Administrators have no way to control users.	Administrators define the access policy

SELinux Configuration files :

- Getenforce
- Sestatus
- Setenforce

Security decisions first go through DAC and then MAC



Linux/Unix Security: Patch/Configs

- Patch management
  - keeping security patches up to date is a widely recognized and critical control for maintaining security
  - application and service configuration
  - most commonly implemented using separate text files for each application and service
  - generally located either in the /etc directory or in the installation tree for a specific application
  - individual user configurations that can override the system defaults are located in hidden “dot” files in each user’s home directory
  - most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

- Users, groups, and permissions
  - access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
  - guides recommend changing the access permissions for critical directories and files
  - local exploit
    - software vulnerability that can be exploited by an attacker to gain elevated privileges
  - remote exploit
    - software vulnerability in a network server that could be triggered by a remote attacker

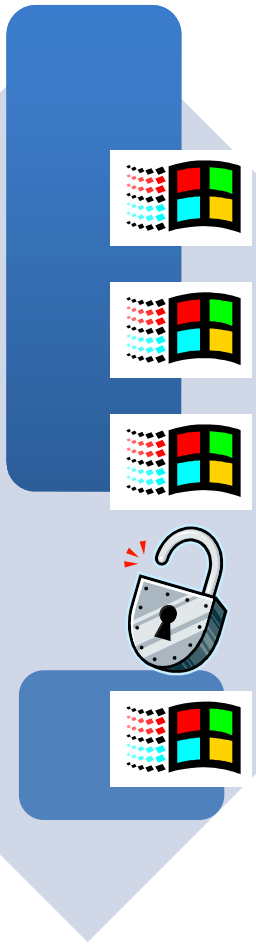
Linux/Unix Security

- Chroot jail
  - restricts the server's view of the file system to just a specified portion
  - uses chroot system call to confine a process by mapping the root of the filesystem to some other directory
  - file directories outside the chroot jail aren't visible or reachable
  - main disadvantage is added complexity

Windows Security

Patch management

- "Windows Update" and "Windows Server Update Service" assist with regular maintenance and should be used
- third party applications also provide automatic update support



Users administration and access controls

- systems implement discretionary access controls resources
- Vista and later systems include mandatory integrity controls
- objects are labeled as being of low, medium, high, or system integrity level
- system ensures the subject's integrity is equal or higher than the object's level
- implements a form of the Biba Integrity model

Windows Security

Much of the configuration information is centralized in the Registry

- Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - more useful for making bulk changes

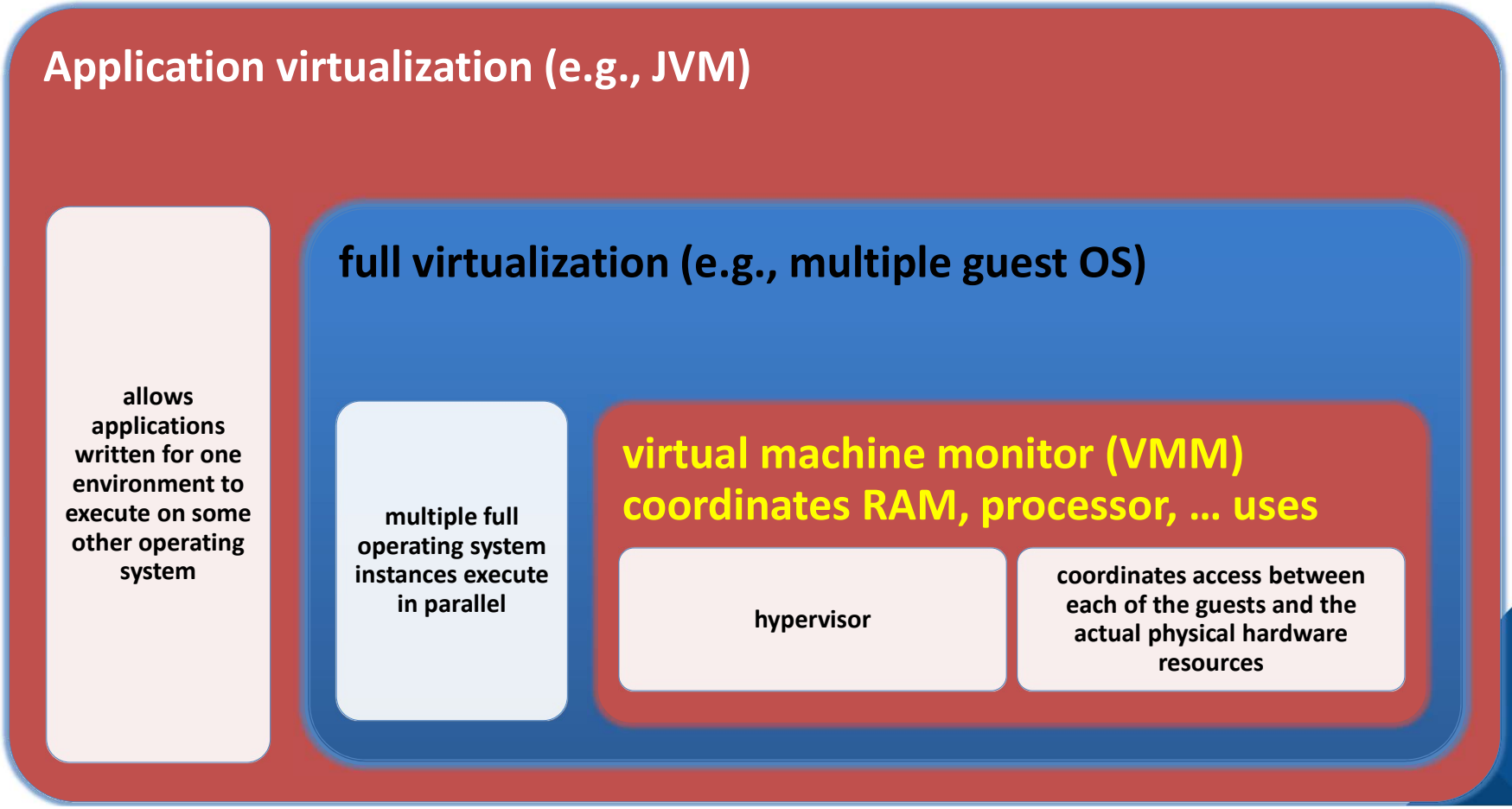
Windows Security

- Other security controls
- Essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
- Current generation Windows systems include basic firewall and malware countermeasure capabilities
- Important to ensure the set of products in use are compatible
- Windows systems also support a range of cryptographic functions:
- Encrypting files and directories using the Encrypting File System (EFS)
- Full-disk encryption with AES using BitLocker
- “Microsoft Baseline Security Analyzer”
- Free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Virtualization

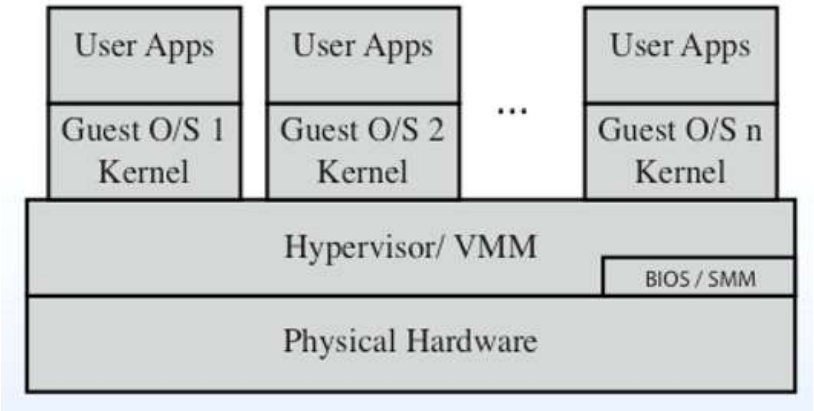
- A technology that provides an abstraction of the resources used by some software which runs in a simulated environment called a virtual machine (VM)
- Benefits include better efficiency in the use of the physical system resources
- Provides support for multiple distinct operating systems and associated applications on one physical system
- Raises additional security concerns

Virtualization Alternatives



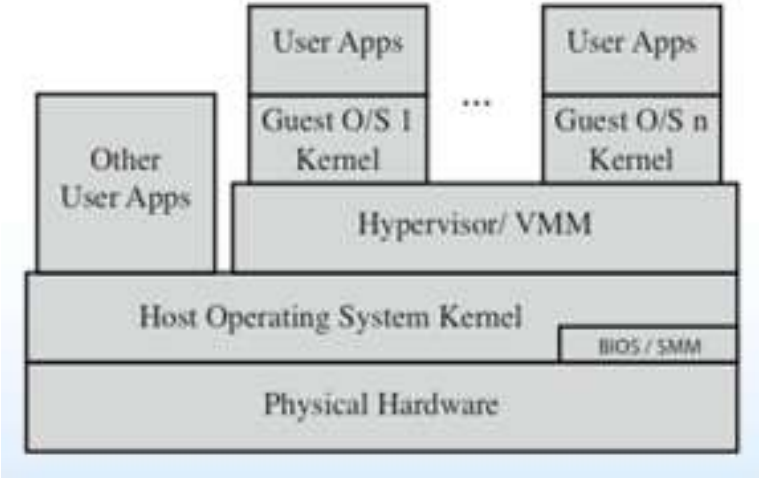
Full Virtualization Variations

- **Native virtualization**: the hypervisor executes directly on the underlying hardware
- Hosted OS is just another app
- More secure: fewer layers



Full Virtualization Variations

- **Hosted virtualization**: Hosted OS run along other apps
- Adds additional layers: increased security concerns



Virtualization Security Issues

- Security concerns include:
  - **Guest OS isolation**: ensuring that programs executing within a guest OS may only access and use the resources allocated to it
  - Guest OS monitoring by the **hypervisor**: has privileged access to the programs and data in each guest OS and ***must be trust***
  - Virtualized environment security: particularly **image** and **snapshot management** which attackers may attempt to view or modify

Hypervisor Security

- Should be
  - secured using a process similar to securing an operating system
  - installed in an isolated environment
  - configured so that it is updated automatically
  - monitored for any signs of compromise
  - accessed only by authorized administration
- May support both local and remote administration so must be configured appropriately
- Remote administration access should be considered and secured in the design of any network firewall and IDS capability in use

We have secured the windows. Good job!

Absolute Security

Absolute Security

Never connect computer to anything and store it in a place that no one can ever find it

Not at all feasible. So how do we secure Windows to the best of our abilities?

General Advice: Drive Encryption

Windows offers BitLocker

- But only available for Pro, Enterprise and Education licensees of Windows 10.

VeraCrypt is a good free 3rd party alternative

General Advice: Strong Passwords

If you have all of the strongest defenses available, but your passwords are weak, your defenses are nearly useless

- Generally minimum 15 characters with mixed case, numbers, and symbols
- Optimal: randomly selected characters → better to find happy medium

Alternative, better solutions (though not always feasible): Key-based login, 2-factor authentication

General Advice: Access Control

Principle of Least Privilege: "Every program and every user of the system should operate using the least set of privileges necessary to complete the job"[1]

Basically, Jill from Corporate Party Planning should not have access production environments, including the files it contains, because she does not need that level of access

General Advice: Regular Backups

Backups of files and systems are important

- Rolling back to a known good state can sometimes be quicker than trying to resolve misconfiguration
  - This does not mean that vulnerabilities should be ignored

Check out Backup Settings (Windows 10) or Backup and Restore (older Windows versions)

General Windows Knowledge

Cmd & Powershell

Cmd: original command line utility (older than dirt), more difficult to use

PowerShell: Command line shell and scripting language, similar to Unix-based shells

- Utilizes Visual Basic/.NET, so possible to create new modules
- Unified interface to interact with system, utilities, and services

Will save many hours of point-and-click if you get comfortable with utilizing PowerShell

Know what is running

It is difficult to secure any computer without knowing what is running on it

Find what programs run on startup in C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

For Windows, utilize PowerShell to view running processes

- *Get-Process*: Lists running processes https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-powershell-1.0/ee176855(v=technet.10)

Get-Process

```
Get-Process | Select-Object name,fileversion,productversion,company
```

```
Name                 FileVersion          ProductVersion       Company
----                 -----------          --------------       -------
alg                  5.1.2600.2180 (x...  5.1.2600.2180        Microsoft Corpor...
apdproxy             3.0.0.53237          3.0.0.53237          Adobe Systems In...
asghost              1.5.0.035            1.5                  Cognizance Corpo...
ati2evxx             6.14.10.4118         6.14.10.4118.02      ATI Technologies...
```

Windows Event Viewer

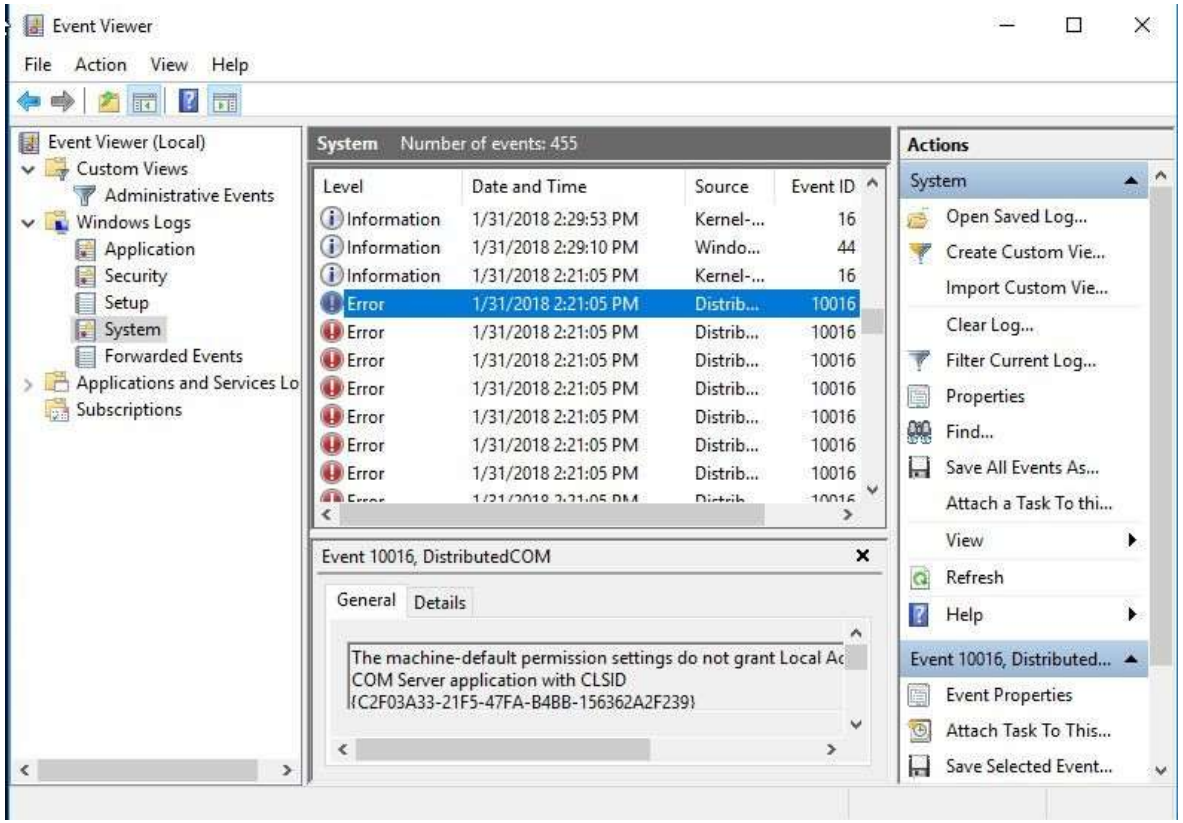
Window's built-in way to view event logs

Beware of lots of information, warnings, and errors

- Information - program reporting information of its execution
- Warning - not necessarily significant, but an issue might be about to occur
- Error - probably a major issue

Default save location: C:\Windows\System32\winevt\Logs\

Windows Event Viewer



Windows Registry

Registry: "a system-defined database in which applications and system components store and retrieve configuration data" [2]

- Stored in a tree structure, up to 512 levels deep

Utilizes standard access control (must have proper privileges to modify certain registry key values)

[2] Microsoft Registry Documentation

Important Windows Registry Keys

- DisallowRun: prevent certain exe files from executing
- fDenyTSConnections: disables Remote Desktop
- restrictanonymoussam: prevent anonymous enumeration of SAM accounts and shares
- RNG\Seed: seed used for random number generation
- HKEY_CLASSES_ROOT*: mapping of all known file extensions to programs

Tin Foil Hats in Windows

How to disable built-in tracking

1. Don’t use your microsoft account as login
   a. “Local account” = less tracked account
2. Disable associated services that keep track of location, what websites you have visited, etc.
3. Limit which apps can utilize camera, location, microphone, etc.

Active Directory

What is Active Directory?

Active Directory - a directory service that keeps track of users and systems within the network

- Utilizes domains - computer network with all user accounts, systems, and security policies registered within a central database

Basically a service that allows administrators of Windows networks to manage users who need the ability to access multiple services/systems across the network

Why do Ineed to know about Active Directory?

Almost every major company and government agency has at least 1 Windows domain that utilizes AD

- For blue or red team roles, being comfortable with Active Directory management can be invaluable
- Windows dominance within the corporate computing industry will not be going away anytime soon

Active Directory Components

Domain Controller: server(s) running the Active Directory Domain Services (AD DS)

- AD DS keeps data in a tree structure that can be accessed using LDAP
- Authentication handled using Kerberos
- Samba for network shares

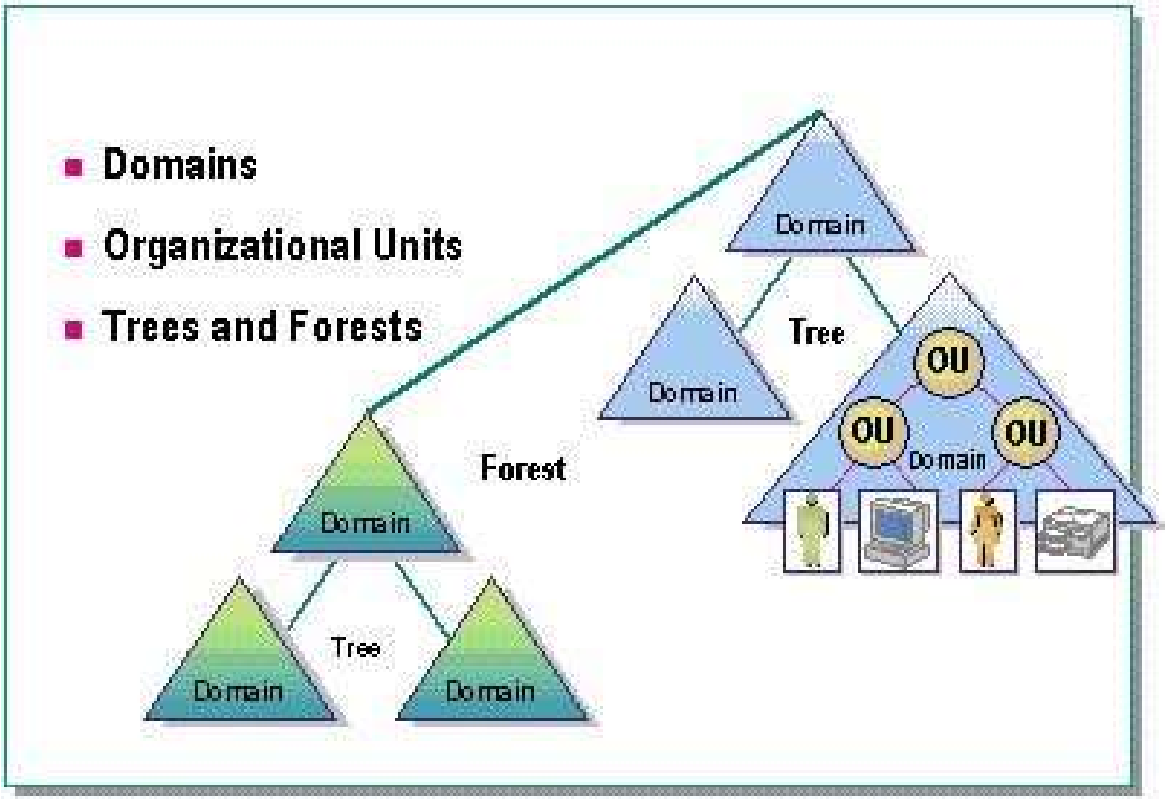
Usually includes DNS server, WSUS, Exchange email server, network shares

Active Directory Structure

Active Directory uses tree structures to keep track of users and the categories they fit in

Active Directory Structure

- Logical Structure



Group Policy

Group policy - centralized management and configuration of user/system accounts

Helps to enforce user/group access control across the network using rules

Group Policy Object - set of Group Policy rules

- Import/Export GPO in order to have standardized rules throughout multiple domains

Group Policy

Group Policy Preferences - settings that are preferred by the admin, but not enforced

CAUTION: The Group Policy Preferences AES key that is used for encrypting passwords within the Preferences Policy file is publicly available through Microsoft

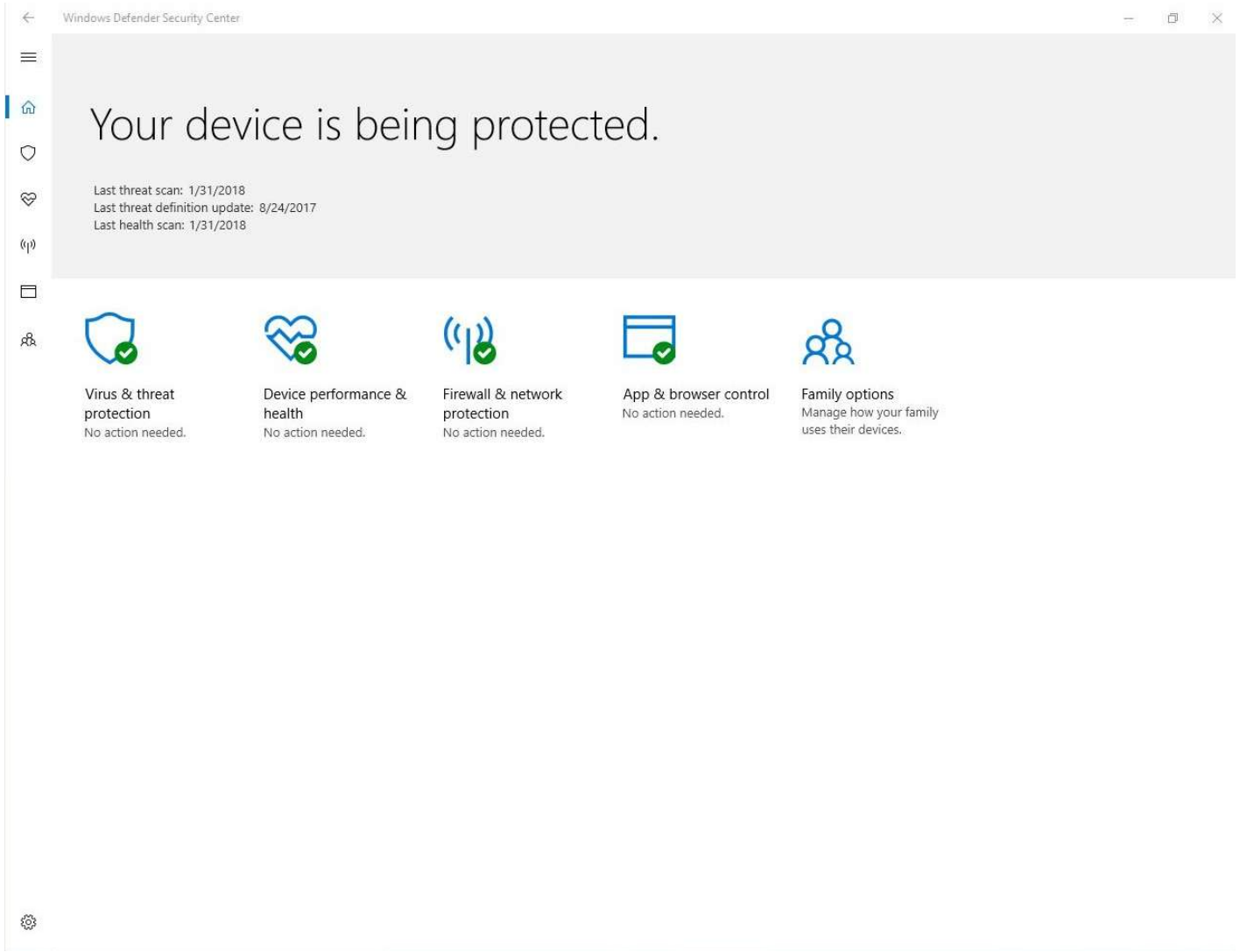
Threat Protection

Updates to Microsoft Security Tools

- Fortunately, Microsoft has updated most of its security suite
- Unfortunately, this means most of the old tools don’t work anymore

Defender Security Center

- Aggregates most security features in a single application
- Firewall
- Antivirus
- Application Protection


Windows Defender Security Center
Your device is being protected.
Last threat scan: 1/31/2018
Last threat definition update: 8/24/2017
Last health scan: 1/31/2018
Virus & threat protection
No action needed.
Device performance & health
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Family options
Manage how your family uses their devices.

Defender Exploit Guard

- New product designed to be close to a built in HIPS System
- Replaces EMET
- Exploit Protection
- Attack Surface reduction
- Network Protection
- Controlled Folder Access

Exploit Protection

- Customizable in Defender Security System
- Data Execution Protection
- Control Flow Guard
- Address Space Layout Randomization
- Various App Level protections

Attack Surface Reduction

- Disables potentially malicious behaviors
- “Block executable content from email client and webmail”
- “Block Office applications from creating child processes”
- No custom rules
- Can be applied in audit and block mode

Network Protection

- Block outgoing traffic to malicious domains
- Can’t pick what domains are on that list
- Can be applied in audit and block mode

Controlled folder access

- Marketed as ransomware protection
- Allows folders to be marked as "protected"
- Protected folders can only be modified by whitelisted programs
- Program whitelist can be configured in Defender Security Center

Windows Defender Playground

https://demo.wd.microsoft.com/

Windows SmartScreen

- Scans websites for malicious behavior
- Scans downloaded files for malicious behavior
- Warns user if anything unusual is detected

Defender Application Guard

- Can’t be run in a VM easily :(
- Windows 10 only
- Runs Internet Explorer/Edge in a HyperV container if the website is untrusted
- Supposedly doesn’t share the kernel

Event Forwarding

- Finally?
- Replaces features provided by Sysmon
- Sends events to a Windows Event Collector


thank you