Course 3 Week 2

Characteristics of Client System Administration ?

What is Client?

→ The Client-Server model describing how a server provides resources to one or more clients.

(one to many relationship.)

Client system administration and Cybersecurity.

→ Cloud & Mobile computing.

→ New Devices, new applications, and new services

→ Endpoint devices are the front line of attack.

Common type of Endpoint attacks:

→ Spear phishing

→ Watering Hole → Malware placed on a site frequently visited by an employee or a group of employee.

→ Ad Network attacks → Using ad networks to place malware on a machine through ad software.

→ Island Hopping → Supply chain Exfiltration.

Endpoint Protection Basics

→ Policy-based approach to network security → Endpoint Protection Management

→ Endpoint security Management Systems, which can be purchased as a software or as dedicated

as a software ...
appliance ...

→ Endpoint Security Systems →
Work on client/server model
in which a centrally managed
server or gateway hosts
the security program
and an accompanying client progra
is installed on each network

Unified Endpoint Management (UEM)

↳ Converges client-based management
techniques with Mobile Device
Management (MDM) application
Programming interfaces (API).

Endpoint Protection & Response.

→ Key mitigation capabilities for endpoint
• Deployment of devices with network

configuration.

- Automatic quarantine/blocking of non-complaint endpoints
- Ability to patch thousands of endpoints at once.

Endpoint Detection & Response.

→ Automatic Policy creation for endpoints

Threat Hunting → Zero-Day OS updates

Detection

Respons → Continous Monitoring, patching & enforcements of security policies

user

Execution Across endpoints.

IBM MaaS 360 with Watson for Cognitive UEM.

Trusted Advisor.

Actionable Insights.
(Apps & content)

Contextual
Insights.
(People & Ident

(Devices & things)

Overview of Patching.

Why Patching?

- All OS require some type of Patching.

→ Patching is fundamental and most important thing an organization can do to prevent malicious attacks.

A patch is a set of changes to a Computer program or its supporting

UAM designed to update, fix or improve it.

Windows Patching.

- Security updates
- Critical updates
- Software updates
- Service Packs

Monthly → Patch Released → Testing → Distribute to organization