

Course 3 Week 2

Characteristics of Client System Administration?

What is Client?

→ The Client server model describing ^{one to many relationship.} how a server provides resources to one or more clients.

Client system administration and Cybersecurity.

→ Cloud & Mobile computing.

→ New Devices, new applications, and new services

→ Endpoint devices are the p
Front line of attack.

• • • • • Attack.

Common type of Endpoint attacks.

→ Spear phishing

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

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

→ Island Hopping → Supply chain Infiltration.

Endpoint Protection Basics

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

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

as a separate ...
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 program
is installed on each network

Unified Endpoint Management (UEM)

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

Endpoint Protection & Response.

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

Configuration.

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

Endpoint Detection & Response.

→ Automatic Policy creation for endpoints

Threat Hunting
Detection

→ Zero-Day OS updates

Response

→ Continuous Monitoring, patching & enforcement of security policies

user education across endpoints.

IBM Max 360 with Watson
for Cognitive UEM.

Trusted Advisor.

Actionable Insights.
(Apps & content)

Contextual
Insights.
(People & Interactions)

(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
data.

UAA designed to update, fix or
improve it.

Windows Patching.

↳ Security updates

↳ Critical updates

↳ Software updates

↳ Service Packs

Monthly ↓

Patch Released → Testing ⇒ Distribute
to organization