Week 2 – Incident Classification

1. Incident Types
2. MITRE ATT&CK Mapping
3. Metadata Fields (Table)

Section 1: Incident Types

- Phishing
- Malware
- Ransomware
- Insider Threat
- DDoS
- Data Exfiltration

Section 2: MITRE ATT&CK Mapping

- T1566 – Phishing
- T1059 – Command & Scripting Execution
- T1204 – User Execution
- T1027 – Obfuscated/Encrypted Files

Section 3: Metadata Table

Field	**Example**
Hostname	WIN-Server-01
Source IP	192.168.1.25
File Hash	98b7c2e41ff9...
Timestamp	2025-08-18 15:22
IOC	crypto_locker.exe
Description	Initial point of analysis
Severity	High
Status	New