Dive into the world of cybersecurity incident detection and response.

Answer Key P1C2

Description	Tactic (ATT&CK)	Technique (ATT&CK)	Detection (D3FEND)
Email address search	Reconnaissance	**T1589.002** : Gather Victim Identity Information: Email Addresses	NA
Phishing with a malicious attachment	[Initial Access]	T1566.001 : [Phishing: Spearphishing Attachment]	**D3-PMAD** : Protocol Metadata Anomaly Detection **D3-HD** : Homoglyph Detection **D3-SMRA** : Sender MTA Reputation Analysis **D3-SRA** : Sender Reputation Analysis
Execution of malware via a malicious macro	Execution	[T1204.002 : User Execution: Malicious File] [T1059.005 : Command and Scripting Interpreter: Visual Basic]	[**D3-DA** : Dynamic Analysis] [**D3-EFA** : Emulated File Analysis] [**D3-FA** : File Analysis]
Exploitation of a vulnerability	Privilege Escalation	T1068 : Exploitation for Privilege Escalation	**D3-SSC** : Shadow Stack Comparisons]

to escalate privileges			**D3-PCSV** : Process Code Segment Verification
Connection to other systems in the network	[Lateral Movement]	T1021 : Remote Services	**D3-NTCD** : Network Traffic Community Deviation
Deployment of ransomware and encryption of Meditroniqu e data	Impact	[T1486 : Data Encrypted for Impact]	NA