Complete the Attack Vectors sheet first to pre-	List detective or preventive solutions associated with TTP.				
populate this column's dropdown! T1203-Explotation for client execution	DS002(File modification)	DETECTIVE: Data source	NO	File Date Co. o.	(orooto)
T1538-Cloud service dashboard	DS002(File modification) DS0002(User account authentication)	DETECTIVE: Data source	NO NO	File, Data Sol Changes made to a file, including updates to its contents, User Account An attempt (successful and failed login attempts) by a user, servi	(create)
T1115-Clipboard data	DS0017(Command execution)	DETECTIVE: Data source	YES		(create)
T1110-Brute force	DS0017(Command execution)	DETECTIVE: Data source	YES	Command, D A directive given to a computer program, acting as an inter-	(create)
T1190-Exploiting public facing application	DS0029(Network traffic content)	DETECTIVE: Data source	YES		(create)
1 31 3 11	DS0029(Network traffic content)		YES	Network Traff The full packet capture (PCAP) or session data that logs b	,
T1595-Active scanning	, ,	DETECTIVE: Data source	YES	Network Traff Summarized network packet data that captures session-level deta	(create)
T1550-Use alternate authentication material	M1047(Audit)	PREVENTIVE: Mitigation		Audit, Mitigati Auditing is the process of recording activity and systematically i	(implement)
T1578-Modify cloud compute infastructure	M1047(Audit)	PREVENTIVE: Mitigation	YES	Auditing is the process of recording activity and systematic	(validate), (maintain)
T1650-Acquire access	M1056 (Pre-compromise)	PREVENTIVE: Mitigation	YES	Pre-comprom Much of this takes place outside the visibility of the target	(implement)
T1586-Compromised accounts	M1056(Pre-compromise)	PREVENTIVE: Mitigation	YES	Pre-comprom Pre-compromise mitigations involve proactive measures a	(implement)
T1584-Compromise Infastructure	M1056(Pre-compromise)	PREVENTIVE: Mitigation	YES	Pre-comprom Pre-compromise mitigations involve proactive measures and defe	(implement)
T1595-Active scanning	M1056(Pre-compromise)	PREVENTIVE: Mitigation	YES	Pre-comprom Pre-compromise mitigations involve proactive measures and defe	(implement)
T1203-Explotation for client execution, T1538- Cloud service dashboard	·	DETECTIVE: Honeypot	YES	Create New C Enticing files or data that alert as soon as opened/accessed/views SI	
T1115-Clipboard data, T1110-Brute force	Honeycreds	DETECTIVE: Honeypot	YES	Create New C Enticing credentials that alert as soon as login attempt occ SI	(create), (ingest alerts into IEM)
T1190-Exploiting public facing application, T1595-Active scanning	Honeypot	DETECTIVE: Honeypot	YES	Create New C Looks like a legitimate device with detectable vulnerabilitie SI	(create), (ingest alerts into IEM)
T1651-Cloud administration command, T1078-Valid accounts	Honeydata	DETECTIVE: Honeypot	YES	Create New C Enticing files or data that alert as soon as opened/accesse SI	(create), (ingest alerts into IEM)

Complete the Attack Vectors sheet first to prepopulate this column's dropdown!	List detective or preventive solutions associated with TTP.			
populate ans columns dropdown:				

Complete the Attack Vectors sheet first to prepopulate this column's dropdown!	List detective or preventive solutions associated with TTP.			
populate tills columns dropdown:				

Complete the Attack Vectors sheet first to prepopulate this column's dropdown!	List detective or preventive solutions associated with TTP.			