

Darktrace:

Mapping to MITRE

DARKTRACE

The MITRE ATT&CK® framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The framework is available to all from the [MITRE website](#), and is used by organizations to help them understand how an adversary launches an attack, correlate adversaries to the specific techniques they use, and evaluate their defenses and strengthen them where it matters most.

MITRE is broken down into several tactics – displayed left to right according to the attack life-cycle – and these are in turn broken down into different techniques, which vary based on the tools an attacker has available, and how an organization’s systems are configured. The framework is constantly being refined and extended as more information is gathered.

/ How Darktrace Maps to MITRE

Darktrace’s Cyber AI Loop reduces risk and enables threat detection and response in the majority of techniques listed in the MITRE ATT&CK framework. From the Model Editor, Darktrace users can download a JSON that can be loaded into the MITRE attack-navigator to show which techniques Darktrace models can detect.

This is summarized here (Figure 1), with a detailed breakdown below.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning Gather Victim Identity Information Gather Victim Network Information Phishing for Information	Compromise Accounts Compromise Infrastructure Develop Capabilities Establish Accounts Obtain Capabilities Stage Capabilities	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Replication Through Removable Media Trusted Relationship Valid Accounts	Command and Scripting Interpreter Container Administration Command Exploitation for Client Execution Inter-Process Communication Scheduled Task/Job Software Deployment Tools System Services User Execution Windows Management Instrumentation	Account Manipulation BITS Jobs Browser Extensions Create Account Create or Modify System Process External Remote Services Modify Authentication Process Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Valid Accounts	Create or Modify System Process Domain Policy Modification Scheduled Task/Job Valid Accounts	BITS Jobs Direct Volume Access Domain Policy Modification File and Directory Permissions Modification Impair Defenses Indicator Removal on Host Masquerading Modify Authentication Process Modify Cloud Compute Infrastructure Pre-OS Boot Rogue Domain Controller System Binary Proxy Execution Use Alternate Authentication Material Valid Accounts

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Adversary-in-the-Middle Brute Force Exploitation for Credential Access Modify Authentication Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal or Forge Kerberos Tickets Steal Web Session Cookie Unsecured Credentials	Account Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Permission Groups Discovery Query Registry Remote System Discovery System Information Discovery System Network Configuration Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material	Adversary-in-the-Middle Audio Capture Automated Collection Browser Session Hijacking Data from Cloud Storage Object Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Web Service	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Endpoint Denial of Service Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot











































The above is a representation of Darktrace’s coverage of every single technique for the full MITRE ATT&CK (v11) matrix for Enterprise. Each organization is unique and will likely not require ticking every box above. To find what’s relevant for your organization, visit [this page](#) for a breakdown of tactics & techniques by coverage area (network, O365, Azure AD, Google Workspace, Windows, etc.). It is possible that Darktrace covers 100% of what is relevant to your organization.

Below is a list of every technique and sub-technique covered specifically by one of Darktrace’s models. It is worth noting that a combination of these models might detect further techniques & sub-techniques than those shown below.

Darktrace is extremely powerful and, in a single pane of glass, is very easy to for me to navigate to find and do what I need to do.

/ Clint Watson, Division Manager of Technology at Australian Grand Prix Corporation


















































* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
O1 Reconnaissance	T1598.003	Spearphishing Link	 Darktrace/Email (1+)
	T1598.001	Spearphishing Service	 Darktrace/Email (1+)
	T1595.002	Vulnerability Scanning	 Anomalous Connection (1+)  Device (7+)  Antigena::Network::Insider Threat (1+)  Anomalous Server Activity (1+)
	T1595.001	Scanning IP Blocks	 Antigena::Network::Insider Threat (1+)  Device (8+)
	T1595.003	Wordlist Scanning	 Device (3+)  Unusual Activity (1+)
	T1598.002	Spearphishing Attachment	 Darktrace/Email (1+)
	T1589.003	Employee Names	 SaaS::Resource (2+)
	T1590.002	DNS	 Device (2+)
O2 Resource Development	T1586	Compromise Accounts	 SaaS::Access (2+)  SaaS::Compromise (1+)  SaaS::Email Nexus (1+)  Compromise (1+)
	T1585	Establish Accounts	 SaaS::Email Nexus (1+)
	T1584.006	Web Services	 IaaS::Unusual Activity (1+)
	T1583.001	Domains	 Device (1+)
	T1583.005	Botnet	 Anomalous Server Activity (1+)  Compromise (1+)
	T1584	Compromise Infrastructure	 Unusual Activity (1+)
	T1588.001	Malware	 Compromise (1+)  Security Integration (2+)  Anomalous File::Internal (1+)  Device (2+),Anomalous File (19+)  Antigena::Network::External Threat (2+)  Anomalous Connection (1+)  Multiple Device Correlations (1+)  Compliance (1+)
	T1587.003	Digital Certificates	 Compromise (1+)
	T1586.003	Cloud Accounts	 SaaS::Admin (3+)  SaaS::Access (3+)  IaaS::Access (1+)  SaaS::Unusual Activity (3+)  IaaS::Admin (1+)
	T1587	Develop Capabilities	 Security Integration (1+)
	T1584.001	Domains	 IaaS::Network (1+)
	T1586.002	Email Accounts	 SaaS::Access (1+)  SaaS::Compromise (2+)  SaaS::Email Nexus (1+)








































* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
O2 Resource Development	T1608.003	Install Digital Certificate	<div><div></div> Anomalous Connection (3+)</div> <div><div></div> IaaS::Compute (1+)</div> <div><div></div> Compliance (1+)</div> <div><div></div> Multiple Device Correlations (1+)</div> <div><div></div> Antigena::Network::Compliance (1+)</div>
	T1608	Stage Capabilities	<div><div></div> Anomalous File::Internal (1+)</div>
	T1585.002	Email Accounts	<div><div></div> SaaS::Email Nexus (1+)</div>
	T1583.006	Web Services	<div><div></div> Compromise (12+)</div>
O3 Initial Access	T1078	Default Accounts	<div><div></div> User (1+)</div> <div><div></div> IaaS::Compliance (1+)</div> <div><div></div> IaaS::Admin (3+)</div> <div><div></div> Compliance (2+)</div>
	T1078.001	Domain Accounts	<div><div></div> SaaS::Compliance (1+)</div> <div><div></div> User (1+)</div> <div><div></div> Compliance (1+)</div> <div><div></div> SaaS::Admin (1+)</div>
	T1078.002	Trusted Relationship	<div><div></div> SaaS::Admin (3+)</div> <div><div></div> Anomalous Connection (2+)</div> <div><div></div> Device (2+)</div> <div><div></div> Compliance (1+)</div>
	T1078.003	Spearphishing Link	<div><div></div> SaaS::Compliance (2+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> Device (1+)</div> <div><div></div> Darktrace/Email (1+)</div> <div><div></div> Email Nexus (1+)</div>
	T1078.004	External Remote Services	<div><div></div> User (1+)</div> <div><div></div> Anomalous Connection (2+)</div> <div><div></div> Compliance (6+)</div>
	T1091	Local Accounts	<div><div></div> Compliance (1+)</div>
	T1133	Drive-by Compromise	<div><div></div> Compromise (1+)</div> <div><div></div> Device (2+)</div> <div><div></div> Anomalous File (12+)</div> <div><div></div> Unusual Activity (1+)</div> <div><div></div> Antigena::Network::External Threat (2+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> Multiple Device Correlations (1+)</div> <div><div></div> Compliance (1+)</div>
	T1189	Spearphishing via Service	<div><div></div> SaaS::Compliance (2+)</div> <div><div></div> Darktrace/Email (1+)</div>
	T1190	Phishing	<div><div></div> SaaS::Resource (1+)</div> <div><div></div> Anomalous Connection (2+)</div> <div><div></div> Antigena::Network::External Threat (1+)</div> <div><div></div> Email Nexus (5+)</div> <div><div></div> SaaS::Email Nexus (1+)</div>
	T1199	Spearphishing Attachment	<div><div></div> SaaS::Compliance (2+)</div> <div><div></div> Darktrace/Email (1+)</div>




* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
03 Initial Access	T1200	Replication Through Removable Media	<div> Compliance (1+)</div>
	T1566	Valid Accounts	<div><div> IaaS::Compliance (1+)</div><div> IaaS::Access (1+)</div><div> Compliance (1+)</div><div> User (4+)</div><div> Antigena::Network::Insider Threat (1+)</div><div> Multiple Device Correlations (1+)</div><div> IaaS::Admin (2+)</div></div>
	T1566.001	Cloud Accounts	<div><div> SaaS::Email Nexus (3+)</div><div> IaaS::Access (4+)</div><div> IaaS::Compliance (3+)</div><div> IaaS::Compute (1+)</div><div> SaaS::Compliance (4+)</div><div> SaaS::Access (9+)</div><div> SaaS::Unusual Activity (10+)</div><div> Security Integration (1+)</div><div> Antigena::SaaS (3+)</div><div> IaaS::Unusual Activity (2+)</div><div> SaaS::Admin (7+)</div><div> SaaS::Compromise (10+)</div><div> IaaS::Admin (9+)</div></div>
	T1566.002	Exploit Public-Facing Application	<div><div> IaaS::Access (1+)</div><div> Device (1+)</div><div> Compliance (10+)</div><div> IaaS::Compute (1+)</div><div> Anomalous File (1+)</div><div> Anomalous Connection (6+)</div><div> Anomalous Server Activity (5+)</div><div> Container (1+)</div></div>
	T1566.003	Hardware Additions	<div><div> Tags (1+)</div><div> Infrastructure (7+)</div><div> Device (5+)</div><div> Anomalous Connection (1+),Unusual Activity (4+)</div></div>
04 Execution	T1072	Software Deployment Tools	<div><div> SaaS::Compliance (1+)</div><div> Anomalous Connection (1+)</div><div> IaaS::Compute (1+)</div></div>
	T1059.001	PowerShell	<div><div> Anomalous Connection (1+)</div><div> Device (2+)</div><div> IaaS::Compute (1+)</div></div>
	T1059.004	Unix Shell	<div><div> IaaS::Compute (1+)</div></div>
	T1059.008	Network Device CLI	<div><div> Anomalous Connection (1+)</div><div> Compliance (1+)</div></div>
	T1059	Command and Scripting Interpreter	<div><div> Device (1+)</div></div>
	T1204.002	Malicious File	<div><div> SaaS::Resource (1+)</div><div> SaaS::Compromise (1+)</div></div>
	T1059.003	Windows Command Shell	<div><div> IaaS::Compute (1+)</div></div>
	T1609	Container Administration Command	<div><div> IaaS::Compute (2+)</div></div>
	T1559.001	Component Object Model	<div><div> Device (3+)</div><div> Unusual Activity (1+)</div></div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
O4 Execution	T1053	Scheduled Task/Job	 Device (1+)
	T1059.006	Python	 IaaS::Compute (1+)
	T1059.007	JavaScript	 IaaS::Compute (1+)
	T1053.005	Scheduled Task	 Device (2+)
	T1204	User Execution	 Compliance (1+)
	T1569.002	Service Execution	 Device (1+)  Unusual Activity (1+)  Compromise (1+)
	T1204.001	Malicious Link	 Email Nexus (5+)
	T1047	Windows Management Instrumentation	 Anomalous Connection (3+)  Device (5+)  Compromise (2+)
	T1204.003	Malicious Image	 IaaS::Unusual Activity (1+)  IaaS::Compute (1+)
	T1203	Exploitation for Client Execution	 Anomalous Connection (5+)  Compliance (1+)
O5 Persistence	T1098.003	Additional Cloud Roles	 SaaS::Admin (1+)  IaaS::Compute (1+)
	T1176	Browser Extensions	 Compromise (5+)
	T1137.005	Outlook Rules	 SaaS::Compliance (1+)  SaaS::Compromise (1+)
	T1078.001	Default Accounts	 User (1+)  IaaS::Compliance (1+)  IaaS::Admin (3+)  Compliance (2+)
	T1078.002	Domain Accounts	 SaaS::Compliance (1+)  User (1+)  Compliance (1+)  SaaS::Admin (1+)
	T1098.002	Additional Email Delegate Permissions	 SaaS::Unusual Activity (3+)  IaaS::Admin (1+)
	T1136	Create Account	 User (2+)
	T1197	BITS Jobs	 Device (1+)
	T1556	Modify Authentication Process	 SaaS::Compliance (2+)  SaaS::Admin (1+)
	T1136.001	Local Account	 Unusual Activity (1+)
	T1547.012	Print Processors	 Anomalous Connection (1+)
	T1542.005	TFTP Boot	 Compliance (1+)
	T1053	Scheduled Task/Job	 Device (1+)

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
05 Persistence	T1542	Pre-OS Boot	 Anomalous Connection (1+)
	T1133	External Remote Services	 User (1+)  Anomalous Connection (2+)  Compliance (6+)
	T1053.005	Scheduled Task	 Device (2+)
	T1505.003	Web Shell	 Anomalous Connection (1+)  Anomalous Server Activity (1+)
	T1078.003	Local Accounts	 Compliance (1+)
	T1037	Boot or Logon Initialization Scripts	 IaaS::Compute (1+)
	T1098	Account Manipulation	 SaaS::Resource (1+)  IaaS::Compliance (1+)  SaaS::Compliance (5+)  SaaS::Admin (8+)  Antigena::Network::External Threat (1+)  SaaS::Unusual Activity (4+)  IaaS::Admin (10+)
	T1078	Valid Accounts	 IaaS::Compliance (1+)  IaaS::Access (1+)  Compliance (1+)  User (4+)  Antigena::Network::Insider Threat (1+)  Multiple Device Correlations (1+)  IaaS::Admin (2+)
	T1543.001	Launch Agent	 Compliance (1+)
	T1136.003	Cloud Account	 SaaS::Admin (1+)  IaaS::Admin (2+)  SaaS::Compliance (1+)
	T1136.002	Domain Account	 User (2+)
	T1078.004	Cloud Accounts	 SaaS::Email Nexus (3+)  IaaS::Access (4+)  IaaS::Compliance (3+)  IaaS::Compute (1+)  SaaS::Compliance (4+)  SaaS::Access (9+)  SaaS::Unusual Activity (10+)  Security Integration (1+)  Antigena::SaaS (3+)  IaaS::Unusual Activity (2+)  SaaS::Admin (7+)  SaaS::Compromise (10+)  IaaS::Admin (9+)
	T1098.001	Additional Cloud Credentials	 SaaS::Admin (1+)  IaaS::Admin (1+)  IaaS::Unusual Activity (1+)

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
06 Privilege escalation	T1484	Domain Policy Modification	<div><div>Device (1+)</div><div>SaaS::Unusual Activity (1+)</div><div>IaaS::Compliance (1+)</div></div>
	T1078.001	Default Accounts	<div><div>User (1+)</div><div>IaaS::Compliance (1+)</div><div>IaaS::Admin (3+)</div><div>Compliance (2+)</div></div>
	T1078.002	Domain Accounts	<div><div>SaaS::Compliance (1+)</div><div>User (1+),Compliance (1+)</div><div>SaaS::Admin (1+)</div></div>
	T1547.012	Print Processors	<div><div>Anomalous Connection (1+)</div></div>
	T1484.001	Group Policy Modification	<div><div>Device (1+)</div></div>
	T1053	Scheduled Task/Job	<div><div>Device (1+)</div></div>
	T1053.005	Scheduled Task	<div><div>Device (2+)</div></div>
	T1078.003	Local Accounts	<div><div>Compliance (1+)</div></div>
	T1037	Boot or Logon Initialization Scripts	<div><div>IaaS::Compute (1+)</div></div>
	T1078	Valid Accounts	<div><div>IaaS::Compliance (1+)</div><div>IaaS::Access (1+)</div><div>Compliance (1+)</div><div>User (4+)</div><div>Antigena::Network::Insider Threat (1+)</div><div>Multiple Device Correlations (1+)</div><div>IaaS::Admin (2+)</div></div>
	T1543.001	Launch Agent	<div><div>Compliance (1+)</div></div>
	T1078.004	Cloud Accounts	<div><div>SaaS::Email Nexus (3+)</div><div>IaaS::Access (4+)</div><div>IaaS::Compliance (3+)</div><div>IaaS::Compute (1+)</div><div>SaaS::Compliance (4+)</div><div>SaaS::Access (9+)</div><div>SaaS::Unusual Activity (10+)</div><div>Security Integration (1+)</div><div>Antigena::SaaS (3+)</div><div>IaaS::Unusual Activity (2+)</div><div>SaaS::Admin (7+)</div><div>SaaS::Compromise (10+)</div><div>IaaS::Admin (9+)</div></div>
	T1548.002	Bypass User Account Control	<div><div>IaaS::Admin (3+)</div></div>
07 Defense Evasion	T1578.004	Revert Cloud Instance	<div><div>IaaS::Compute (1+)</div></div>
	T1550.003	Pass the Ticket	<div><div>User (1+)</div></div>
	T1484	Domain Policy Modification	<div><div>Device (1+)</div><div>SaaS::Unusual Activity (1+)</div><div>IaaS::Compliance (1+)</div></div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
07 Defense Evasion	T1078.001	Default Accounts	<div><div>User (1+)</div><div>laaS::Compliance (1+)</div><div>laaS::Admin (3+)</div><div>Compliance (2+)</div></div>
	T1562.001	Disable or Modify Tools	<div><div>laaS::Admin (1+)</div></div>
	T1078.002	Domain Accounts	<div><div>SaaS::Compliance (1+)</div><div>User (1+),Compliance (1+)</div><div>SaaS::Admin (1+)</div></div>
	T1578.003	Delete Cloud Instance	<div><div>laaS::Compute (5+)</div></div>
	T1578.002	Create Cloud Instance	<div><div>laaS::Storage (2+)</div><div>laaS::Unusual Activity (1+)</div><div>laaS::Compute (2+)</div></div>
	T1070.008	Clear Mailbox Data	<div><div>SaaS::Resource (2+)</div></div>
	T1222	File and Directory Permissions Modification	<div><div>SaaS::Resource (1+)</div></div>
	T1218.005	Mshta	<div><div>Anomalous File (1+)</div></div>
	T1197	BITS Jobs	<div><div>Device (1+)</div></div>
	T1556	Modify Authentication Process	<div><div>SaaS::Compliance (2+)</div><div>SaaS::Admin (1+)</div></div>
	T1550	Use Alternate Authentication Material	<div><div>SaaS::Admin (1+)</div><div>Device (1+)</div><div>laaS::Compliance (1+)</div></div>
	T1562	Impair Defenses	<div><div>SaaS::Admin (2+)</div><div>laaS::Admin (1+)</div><div>laaS::Compliance (2+)</div><div>User::Key User (1+)</div></div>
	T1036.003	Rename System Utilities	<div><div>SaaS::Resource (1+)</div><div>Unusual Activity (1+)</div></div>
	T1036.007	Double File Extension	<div><div>Anomalous File::Internal (1+)</div></div>
	T1542.005	TFTP Boot	<div><div>Compliance (1+)</div></div>
	T1484.001	Group Policy Modification	<div><div>Device (1+)</div></div>
	T1027.005	Indicator Removal from Tools	<div><div>laaS::Compliance (1+)</div></div>
	T1542	Pre-OS Boot	<div><div>Anomalous Connection (1+)</div></div>
	T1006	Direct Volume Access	<div><div>Device (1+)</div></div>
	T1036.005	Match Legitimate Name or Location	<div><div>Device (1+)</div></div>
	T1562.007	Disable or Modify Cloud Firewall	<div><div>laaS::Compute (1+)</div><div>laaS::Network (9+)</div></div>






























* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
07 Defense Evasion	T1550.001	Application Access Token	<div><div></div> SaaS::Admin (6+)</div> <div><div></div> SaaS::Access (1+)</div> <div><div></div> SaaS::Unusual Activity (1+)</div>
	T1078.003	Local Accounts	<div><div></div> Compliance (1+)</div>
	T1207	Rogue Domain Controller	<div><div></div> Anomalous Connection (2+)</div> <div><div></div> Device (2+)</div> <div><div></div> Anomalous Server Activity (1+)</div>
	T1218.001	Compiled HTML File	<div><div></div> Anomalous File (1+)</div>
	T1550.002	Pass the Hash	<div><div></div> User (2+)</div>
	T1078	Valid Accounts	<div><div></div> IaaS::Compliance (1+)</div> <div><div></div> IaaS::Access (1+)</div> <div><div></div> Compliance (1+)</div> <div><div></div> User (4+),Antigena::Network::Insider Threat (1+)</div> <div><div></div> Multiple Device Correlations (1+)</div> <div><div></div> IaaS::Admin (2+)</div>
	T1564.008	Email Hiding Rules	<div><div></div> SaaS::Compliance (1+)</div> <div><div></div> SaaS::Compromise (1+)</div>
	T1078.004	Cloud Accounts	<div><div></div> SaaS::Email Nexus (3+)</div> <div><div></div> IaaS::Access (4+)</div> <div><div></div> IaaS::Compliance (3+)</div> <div><div></div> IaaS::Compute (1+)</div> <div><div></div> SaaS::Compliance (4+)</div> <div><div></div> SaaS::Access (9+)</div> <div><div></div> SaaS::Unusual Activity (10+)</div> <div><div></div> Security Integration (1+)</div> <div><div></div> Antigena::SaaS (3+)</div> <div><div></div> IaaS::Unusual Activity (2+)</div> <div><div></div> SaaS::Admin (7+)</div> <div><div></div> SaaS::Compromise (10+)</div> <div><div></div> IaaS::Admin (9+)</div>
	T1070.004	File Deletion	<div><div></div> Unusual Activity (1+)</div>
	T1070	Indicator Removal	<div><div></div> SaaS::Resource (1+)</div> <div><div></div> IaaS::Storage (1+)</div> <div><div></div> SaaS::Compromise (1+)</div>
	T1578.001	Create Snapshot	<div><div></div> IaaS::Storage (2+)</div> <div><div></div> IaaS::Compute (1+)</div>
	T1562.008	Disable Cloud Logs	<div><div></div> SaaS::Admin (1+)</div> <div><div></div> IaaS::Compliance (2+)</div>
	T1578	Modify Cloud Compute Infrastructure	<div><div></div> IaaS::Network (2+)</div> <div><div></div> IaaS::Compute (4+)</div>
	T1036	Masquerading	<div><div></div> Anomalous File::Internal (2+)</div> <div><div></div> Anomalous File (1+)</div>
	T1548.002	Bypass User Account Control	<div><div></div> IaaS::Admin (3+)</div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
O8 Credential Access	T1110	Brute Force	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> Device (7+)</div> <div><div></div> Unusual Activity (3+)</div> <div><div></div> SaaS::Access (6+)</div> <div><div></div> SaaS::Compromise (2+)</div> <div><div></div> User (2+)</div> <div><div></div> Anomalous Server Activity (1+)</div>
	T1212	Exploitation for Credential Access	<div><div></div> User (1+)</div> <div><div></div> IaaS::Access (1+)</div>
	T1040	Network Sniffing	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> Compliance (4+)</div>
	T1558.004	AS-REP Roasting	<div><div></div> Compliance (1+)</div>
	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	<div><div></div> User (1+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> Compliance (2+)</div> <div><div></div> Anomalous Server Activity (1+)</div>
	T1556	Modify Authentication Process	<div><div></div> SaaS::Compliance (2+)</div> <div><div></div> SaaS::Admin (1+)</div>
	T1552.005	Cloud Instance Metadata API	<div><div></div> IaaS::Access (3+)</div> <div><div></div> Container (2+)</div> <div><div></div> IaaS::Compute (1+)</div>
	T1558	Steal or Forge Kerberos Tickets	<div><div></div> Device (2+)</div>
	T1110.004	Credential Stuffing	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> SaaS::Access (3+)</div> <div><div></div> IaaS::Access (1+)</div> <div><div></div> Device (2+)</div> <div><div></div> SaaS::Compromise (1+)</div>
	T1558.002	Silver Ticket	<div><div></div> Device (1+)</div>
	T1003.006	DCSync	<div><div></div> Unusual Activity (1+)</div> <div><div></div> Compromise (2+)</div>
	T1110.003	Password Spraying	<div><div></div> SaaS::Access (4+)</div> <div><div></div> SaaS::Compromise (1+)</div> <div><div></div> Device (2+),User (1+)</div> <div><div></div> SaaS::Unusual Activity (1+)</div>
	T1558.003	Kerberoasting	<div><div></div> Compliance (4+)</div>
	T1110.002	Password Cracking	<div><div></div> SaaS::Access (5+)</div> <div><div></div> Anomalous Connection (2+)</div> <div><div></div> Device (2+),User (1+)</div>
	T1539	Steal Web Session Cookie	<div><div></div> SaaS::Access (1+)</div> <div><div></div> SaaS::Unusual Activity (1+)</div>
	T1621	Multi-Factor Authentication Request Generation	<div><div></div> SaaS::Access (1+)</div> <div><div></div> SaaS::Compromise (1+)</div> <div><div></div> Device (2+)</div> <div><div></div> SaaS::Unusual Activity (2+)</div>













































* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
O8 Credential Access	T1552.004	Private Keys	 Device (1+)
	T1557	Adversary-in-the-Middle	 Anomalous Connection (1+)  Device (2+)
	T1528	Steal Application Access Token	 SaaS::Admin (4+)  IaaS::Access (1+)
	T1552	Unsecured Credentials	 Device (1+)
	T1552.006	Group Policy Preferences	 Device (1+)
	T1003.003	NTDS	 Device (1+)  Compromise (2+)
	T1110.001	Password Guessing	 SaaS::Access (5+)  Anomalous Connection (1+)  Device (3+)  User (1+)  Unusual Activity (1+)
	T1558.001	Golden Ticket	 Device (2+)
	T1552.007	Container API	 IaaS::Access (1+)  Container (2+)
	T1552.001	Credentials In Files	 Anomalous File::Internal (1+)  Compliance (1+)
O9 Discovery	T1613	Container and Resource Discovery	 SaaS::Resource (1+)  IaaS::Unusual Activity (1+)
	T1016	System Network Configuration Discovery	 Device (1+)
	T1012	Query Registry	 Device (1+)
	T1526	Cloud Service Discovery	 SaaS::Resource (1+)  IaaS::Access (2+)  IaaS::Unusual Activity (3+)
	T1580	Cloud Infrastructure Discovery	 IaaS::Access (1+)
	T1087.002	Domain Account	 Device (2+)
	T1046	Network Service Discovery	 Anomalous Connection (2+)  Device (13+)  Container (3+)  Unusual Activity (3+)  Antigena::Network::Insider Threat (1+)
	T1040	Network Sniffing	 Anomalous Connection (1+)  Compliance (4+)
	T1135	Network Share Discovery	 Anomalous Connection (1+)  Device (2+)  Antigena::Network::Insider Threat (1+)  Unusual Activity (2+)

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
09 Discovery	T1082	System Information Discovery	<div><div></div> IaaS::Access (1+)</div> <div><div></div> Device (1+)</div> <div><div></div> IaaS::Unusual Activity (1+)</div>
	T1201	Password Policy Discovery	<div><div></div> Container (1+)</div>
	T1018	Remote System Discovery	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> Device (1+)</div> <div><div></div> Antigena::Network::Insider Threat (1+)</div>
	T1087.004	Cloud Account	<div><div></div> SaaS::Resource (2+)</div> <div><div></div> SaaS::Admin (2+)</div> <div><div></div> SaaS::Access (1+)</div> <div><div></div> IaaS::Access (1+)</div>
	T1482	Domain Trust Discovery	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> Device (6+)</div>
	T1615	Group Policy Discovery	<div><div></div> Device (1+)</div>
	T1087	Account Discovery	<div><div></div> Device (3+)</div>
	T1069.003	Cloud Groups	<div><div></div> IaaS::Unusual Activity (1+)</div>
	T1069.002	Domain Groups	<div><div></div> Device (1+)</div>
	T1083	File and Directory Discovery	<div><div></div> Antigena::Network::Insider Threat (1+)</div> <div><div></div> Device (3+)</div> <div><div></div> Compliance (1+)</div> <div><div></div> Unusual Activity (3+)</div> <div><div></div> User (1+)</div> <div><div></div> Anomalous Connection (3+)</div>
	T1538	Cloud Service Dashboard	<div><div></div> SaaS::Resource (1+)</div> <div><div></div> SaaS::Access (2+)</div> <div><div></div> IaaS::Admin (1+)</div> <div><div></div> SaaS::Unusual Activity (2+)</div> <div><div></div> IaaS::Unusual Activity (1+)</div>
10 Lateral Movement	T1072	Software Deployment Tools	<div><div></div> SaaS::Compliance (1+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> IaaS::Compute (1+)</div>
	T1210	Exploitation of Remote Services	<div><div></div> Device (19+)</div> <div><div></div> Compromise (2+)</div> <div><div></div> Multiple Device Correlations (1+)</div> <div><div></div> Anomalous Connection (4+)</div> <div><div></div> Anomalous Server Activity (1+)</div> <div><div></div> Compliance (1+)</div>
	T1550.003	Pass the Ticket	<div><div></div> User (1+)</div>
	T1021.001	Remote Desktop Protocol	<div><div></div> Anomalous Connection (5+)</div> <div><div></div> Device (1+)</div> <div><div></div> Compliance (2+)</div>
	T1534	Internal Spearphishing	<div><div></div> SaaS::Email Nexus (1+)</div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
10 Lateral Movement	T1563.002	RDP Hijacking	<div> Device (1+)</div>
	T1550	Use Alternate Authentication Material	<div><div> SaaS::Admin (1+)</div><div> Device (1+)</div><div> IaaS::Compliance (1+)</div></div>
	T1021.006	Windows Remote Management	<div><div> Anomalous Connection (2+)</div><div> Device (1+)</div></div>
	T1563.001	SSH Hijacking	<div> Anomalous Connection (1+)</div>
	T1021	Remote Services	<div><div> Anomalous Connection (1+)</div><div> Compliance (2+)</div><div> Antigena::Network::Insider Threat (1+)</div></div>
	T1550.001	Application Access Token	<div><div> SaaS::Admin (6+)</div><div> SaaS::Access (1+)</div><div> SaaS::Unusual Activity (1+)</div></div>
	T1080	Taint Shared Content	<div><div> Anomalous Connection (2+)</div><div> Antigena::Network::External Threat (1+)</div><div> Anomalous File::Internal (3+)</div><div> Compliance (1+)</div><div> Compromise (1+)</div></div>
	T1091	Replication Through Removable Media	<div> Compliance (1+)</div>
	T1570	Lateral Tool Transfer	<div><div> Security Integration (1+)</div><div> Anomalous File::Internal (8+)</div><div> Device (2+)</div><div> Compliance (1+)</div><div> Antigena::Network::External Threat (1+)</div><div> Compliance::FTP (2+)</div><div> Antigena::Network::Insider Threat (1+)</div><div> Compromise (2+)</div></div>
	T1550.002	Pass the Hash	<div> User (2+)</div>
	T1021.002	SMB/Windows Admin Shares	<div><div> Anomalous Connection (1+)</div><div> Device (3+)</div><div> Compliance (2+)</div><div> Antigena::Network::Insider Threat (1+)</div></div>
	T1021.003	Distributed Component Object Model	<div> Device (4+)</div>
11 Collection	T1074	Data Staged	<div><div> SaaS::Resource (1+)</div><div> Unusual Activity (5+)</div><div> SaaS::Teams Healthcare (1+)</div><div> Compliance::CCPA and GDPR (1+)</div><div> Anomalous Connection (4+)</div><div> Compliance::FTP (1+)</div><div> Anomalous Server Activity (1+)</div><div> Compliance (1+)</div></div>
	T1025	Data from Removable Media	<div> Compliance (1+)</div>
	T1213.003	Code Repositories	<div> Device (2+)</div>
	T1123	Audio Capture	<div> SaaS::Compliance (1+)</div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
11 Collection	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	<ul style="list-style-type: none"> User (1+) Anomalous Connection (1+) Compliance (2+) Anomalous Server Activity (1+)
	T1119	Automated Collection	<ul style="list-style-type: none"> Unusual Activity (1+)
	T1213	Data from Information Repositories	<ul style="list-style-type: none"> SaaS::Compliance (1+) IaaS::Compliance (1+)
	T1114.003	Email Forwarding Rule	<ul style="list-style-type: none"> SaaS::Admin (1+)
	T1185	Browser Session Hijacking	<ul style="list-style-type: none"> Anomalous Connection (1+) Compromise (1+)
	T1530	Data from Cloud Storage	<ul style="list-style-type: none"> SaaS::Resource (9+) IaaS::Access (2+) IaaS::Compliance (3+) SaaS::Teams Healthcare (4+) IaaS::Storage (3+) SaaS::Compliance (1+) SaaS::Unusual Activity (1+) IaaS::Compute (1+) IaaS::Admin (1+)
	T1005	Data from Local System	<ul style="list-style-type: none"> Container (1+)
	T1039	Data from Network Shared Drive	<ul style="list-style-type: none"> Anomalous Connection (1+)
	T1113	Screen Capture	<ul style="list-style-type: none"> Compliance (1+)
	T1557	Adversary-in-the-Middle	<ul style="list-style-type: none"> Anomalous Connection (1+) Device (2+)
	T1114	Email Collection	<ul style="list-style-type: none"> SaaS::Admin (1+) Unusual Activity (1+)
	T1114.002	Remote Email Collection	<ul style="list-style-type: none"> SaaS::Compliance (1+)
	T1213.002	Sharepoint	<ul style="list-style-type: none"> SaaS::Resource (8+) SaaS::Access (2+) IaaS::Access (2+) IaaS::Compliance (1+)
	T1125	Video Capture	<ul style="list-style-type: none"> SaaS::Compliance (1+)
12 Command and Control	T1092	Communication Through Removable Media	<ul style="list-style-type: none"> Device::Point of Sale (1+) Compliance (1+)
	T1573	Encrypted Channel	<ul style="list-style-type: none"> Anomalous Connection (1+) Compromise (5+)
	T1071.004	DNS	<ul style="list-style-type: none"> Unusual Activity (1+) Compromise::DNS (2+) Device (2+) Anomalous Server Activity (1+) Compromise (8+)









* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
12 Command and Control	T1102	Web Service	<div><div></div> Container (1+)</div> <div><div></div> Compliance::Social Media (1+)</div>
	T1090.003	Multi-hop Proxy	<div><div></div> Antigena::Network::External Threat (1+)</div> <div><div></div> Compromise (6+)</div>
	T1573.001	Symmetric Cryptography	<div><div></div> Compliance (2+)</div>
	T1568.002	Domain Generation Algorithms	<div><div></div> Inoculation (1+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> Anomalous Server Activity (1+)</div> <div><div></div> Compromise (8+)</div>
	T1095	Non-Application Layer Protocol	<div><div></div> Anomalous Connection (4+)</div> <div><div></div> Device (3+)</div> <div><div></div> Unusual Activity (1+)</div>
	T1071	Application Layer Protocol	<div><div></div> Security Integration (1+)</div> <div><div></div> Inoculation::Sinkhole (3+)</div> <div><div></div> Compliance (1+)</div> <div><div></div> Device (5+)</div> <div><div></div> Inoculation::Behavioural (1+)</div> <div><div></div> Anomalous Connection (2+)</div> <div><div></div> Antigena::Network::External Threat (1+)</div> <div><div></div> Compromise (7+)</div>
	T1104	Multi-Stage Channels	<div><div></div> Compromise (3+)</div>
	T1572	Protocol Tunneling	<div><div></div> Unusual Activity (1+)</div> <div><div></div> Anomalous Connection (4+)</div> <div><div></div> Compromise::DNS (8+)</div> <div><div></div> Compliance (2+)</div> <div><div></div> Compromise (1+)</div>
	T1568.001	Fast Flux DNS	<div><div></div> Anomalous Server Activity (1+)</div> <div><div></div> Compromise (5+)</div>
	T1105	Ingress Tool Transfer	<div><div></div> Antigena::Network::External Threat (1+)</div> <div><div></div> Anomalous File (5+)</div> <div><div></div> Compromise (1+)</div> <div><div></div> Compromise::Ransomware (1+)</div>
	T1571	Non-Standard Port	<div><div></div> Anomalous Connection (7+)</div> <div><div></div> Device (2+)</div> <div><div></div> Device::Point of Sale (1+)</div> <div><div></div> Compromise (7+)</div>
	T1102.003	One-Way Communication	<div><div></div> Inoculation (1+)</div> <div><div></div> Container (1+)</div> <div><div></div> Compromise (1+)</div>
	T1219	Remote Access Software	<div><div></div> Anomalous Connection (2+)</div> <div><div></div> Compliance (2+)</div>
	T1001	Data Obfuscation	<div><div></div> Anomalous Connection (3+)</div> <div><div></div> Compromise::DNS (2+)</div> <div><div></div> Anomalous Server Activity (1+)</div> <div><div></div> Unusual Activity (2+)</div>

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
12 Command and Control	T1008	Fallback Channels	 Compromise (4+)
	T1132.001	Standard Encoding	 Anomalous Connection (1+)
	T1090.002	External Proxy	 Anomalous Connection (1+)  Compliance (1+)
	T1090	Proxy	 Infrastructure (1+)
	T1071.001	Web Protocols	 Inoculation (1+)  Inoculation::Behavioural (1+)  Anomalous Connection (12+)  Device (4+)  Compromise (29+)
13 Exfiltration	T1011	Exfiltration Over Other Network Medium	 Unusual Activity (1+)
	T1041	Exfiltration Over C2 Channel	 Antigena::Network::Insider Threat (1+)  Compliance (1+)  Unusual Activity (4+)  Compliance::CCPA and GDPR (1+)  Anomalous Connection (5+)  Compromise (1+)  Anomalous File (1+)
	T1030	Data Transfer Size Limits	 Anomalous Connection (2+)  Antigena::Network::Insider Threat (1+)  Unusual Activity (1+)
	T1052	Exfiltration Over Physical Medium	 SaaS::Resource (1+)
	T1537	Transfer Data to Cloud Account	 SaaS::Resource (9+)  SaaS::Email Nexus (1+)  IaaS::Compliance (1+)  IaaS::Storage (2+)  SaaS::Compliance (1+)  Compliance::File Storage (5+)  Compliance (1+)  Antigena::Network::Compliance (1+)
	T1020.001	Traffic Duplication	 IaaS::Compliance (1+)
	T1048.003	Exfiltration Over Unencrypted Non-C2 Protocol	 Compliance::FTP (3+)  Compromise::DNS (3+)  Device (1+)  Compromise (1+)  Compliance (1+)
	T1048	Exfiltration Over Alternative Protocol	 SaaS::Email Nexus (2+)  Anomalous Connection (2+)  Device (1+)
	T1567	Exfiltration Over Web Service	 SaaS::Resource (5+)  SaaS::Email Nexus (1+)  Compliance::File Storage (1+)  Compliance (3+)
	T1029	Scheduled Transfer	 Anomalous Connection (1+)

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
13 Exfiltration	T1052.001	Exfiltration over USB	 Compliance (1+)
	T1020	Automated Exfiltration	 Anomalous Connection (2+)
	T1567.002	Exfiltration to Cloud Storage	 SaaS::Resource (1+)  Anomalous Connection (2+)  Compliance::File Storage (9+)  Unusual Activity (3+)  Antigena::Network::Compliance (1+)
14 Impact	T1499.001	OS Exhaustion Flood	 Device (1+),  Anomalous Server Activity (1+)
	T1565.001	Stored Data Manipulation	 IaaS::Storage (1+)  SaaS::Resource (1+)  IaaS::Compliance (1+)  SaaS::Teams Healthcare (1+)
	T1498.001	Direct Network Flood	 Anomalous Server Activity (1+)  IaaS::Network (2+)
	T1491.002	External Defacement	 IaaS::Compute (1+)
	T1498.002	Reflection Amplification	 Anomalous Server Activity (1+)
	T1499.004	Application or System Exploitation	 Anomalous Connection (1+)  Device (1+)  IaaS::Network (2+)
	T1485	Data Destruction	 SaaS::Resource (7+)  IaaS::Unusual Activity (2+)  SaaS::Teams Healthcare (1+)  IaaS::Storage (2+)  SaaS::Compromise (1+)  Unusual Activity (1+)
	T1565	Data Manipulation	 IaaS::Admin (1+)
	T1496	Resource Hijacking	 Compliance (1+)  Antigena::Network::External Threat (1+)  Compromise (3+)  IaaS::Compute (3+)  IaaS::Unusual Activity (1+)
	T1491.001	Internal Defacement	 IaaS::Compute (1+)
	T1499.002	Service Exhaustion Flood	 Compliance (1+)  Anomalous Server Activity (1+)
	T1499.003	Application Exhaustion Flood	 SaaS::Compliance (1+)  Compliance (1+)  Anomalous Server Activity (1+)
	T1531	Account Access Removal	 User (1+)
	T1489	Service Stop	 Anomalous Connection (2+)

* Includes Sub-Techniques

Tactic	Technique* ID	Technique* Name	Darktrace AI Model Folders
14 Impact	T1529	System Shutdown/Reboot	<div><div></div> Anomalous Connection (1+)</div> <div><div></div> Device (3+)</div> <div><div></div> Anomalous Server Activity (2+)</div>
	T1486	Data Encrypted for Impact	<div><div></div> SaaS::Resource (2+)</div> <div><div></div> Security Integration (2+)</div> <div><div></div> Anomalous Connection (1+)</div> <div><div></div> Compromise::Ransomware (9+)</div> <div><div></div> Unusual Activity (4+)</div> <div><div></div> Antigena::Network::External Threat (2+)</div> <div><div></div> SaaS::Compromise (1+)</div>

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.



Scan to
LEARN MORE

DARKTRACE

Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

Latin America: +55 11 97242 2011

info@darktrace.com

[in](#) [twitter](#) [youtube](#)
darktrace.com