Threat Name: Enterprise ATT&CK
Threat ID: x-mitre-collection--23320f4-22ad-8467-3b73-ed0c869a12838
Description: ATT&CK for Enterprise provides a knowledge base of real-world adversary behavior targeting traditional enterprise networks. ATT&CK for Enterprise covers the following platforms: Windows, macOS, Linux, PRE, Office 365, Google Workspace, IaaS, Network, and Containers.
Created by: identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
Date Created: 2018-01-17T12:56:55.080Z
Date Modified: 2018-01-17T12:56:55.080Z
Platforms: Not Specified
Spec version: 2.1
Kill chain: null
Threat Name: Application Deployment Software Mitigation
Threat ID: course-of-action--c88151a5-fe3f-4773-8147-d801587065a4
Description: Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through Exploitation of Vulnerability.

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.
Created by: identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
Date Created: 2018-01-17T12:56:55.080Z
Date Modified: 2018-01-17T12:56:55.080Z
Platforms: Not Specified
Spec version: 2.1
Kill chain: null