Cyber Yankee 21 ROE

All entries on the CY21 No Strike List are out of play and should not be blocked, deleted, or modified by Blue Teams.

Range-isms:

All Range VMs are dual homed, with one network interface connected to the 10.10.0.0/16 network for simulated user control. This 10.10.0.0/16 network is out of play.

Every 30 minutes the range automation will reset the following settings:

* Simulated user account passwords
* Routes and Firewall Rules
* Workstation Active Directory Domain membership
* Email configuration
* Windows VM IP addresses and hostnames

When approved by the change Management Process to block IP Addresses, only individual IP Address may be blocked (x.x.x.x/32). Blue Teams will not block entire subnets. Blue teams may be authorized to implement Firewall rules to block individual /32 IP addresses, but these changes will be automatically reverted by range automation. To make the Firewall rule changes permanent, the Blue Team will need to submit a Change Request to the Range Team in DefenderLogs inside of PCTE requesting the change.

To maintain the simulated user traffic, Blue Teams are not to change passwords for simulated user accounts. When a user account has been confirmed to have a compromised password, the Blue Team can submit a Change Request to the Range Team in DefenderLogs inside of PCTE requesting that the user password be changed. The request will have the compromised user account(s) and a justification for the password change. The password change will be implemented by the Range Team.

Accounts associated with malicious activity may be disabled with the approval of the Enclave Designated Approval Authority (DAA) following the Change Management Process.

**User Emulation**

Metova User Emulation processes (used for traffic generation) should not be terminated by Blue Team. User emulation is not an external control harness; instead it operates on each host which emulates a working end-user. Because of this, there are several visible artifacts on a virtual network that should be ignored by defense teams.

The user emulation servers and their agents communicate via AMQP on TCP port 5672 using the control subnet of the virtual network. As with the control network generally, no traffic should be blocked or flagged as suspicious. Host-based security in particular should be configured to allow all traffic on the control subnet interface.

The agents on each host uses two processes which communicate with each other using a bidirectional RPC service on TCP port 49998 and 49999 using the loopback network interface 127.0.0.1. Like the AMQP traffic on the control subnet, this traffic on the loopback network should not be blocked or flagged as suspicious by host-based security tools.

When running on a host, the user emulation system spawns two or three processes in addition to the user applications such as Outlook or Word:

• The command and control process, also known as C2. This process is a Java program and runs as java.exe or javaw.exe. It communicates with the UE server via AMQP and communicates with the actuation process as described in the previous section. It is started with the system and is installed as a Windows service.

• The actuation process. This process is a Java program as well and also runs as java.exe or javaw.exe. It is launched by the launcher script run-actuation.cmd or ueactuation.cmd and those scripts are configured to be started automatically when users log into a host. Note: Actuation will never run for users with admin in their name.

• A web browser driver process used as an intermediary to control browser behavior. Which process is spawned depends on the browser configured: chromedriver.exe for Chrome, IEDriverServer.exe for Internet Explorer. Firefox does not spawn an additional driver process.

The actuation process is the process which controls other applications in order to emulate activities. How it spawns and controls those other applications varies based on the activity:

• For activities using a web browser such as web browsing, Sharepoint, and social networking the actuator launches and controls the web browser using Selenium and WebDriver, an industry standard browser automation system. This control may present additional artifacts in the form of TCP connections over port 127.0.0.1.

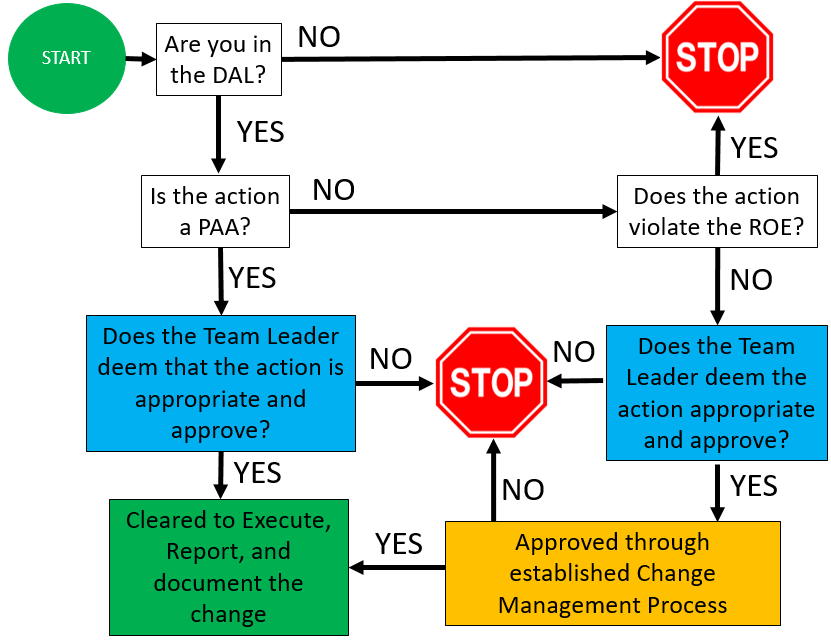
• For activities using Microsoft Office applications including Outlook, Word, Powerpoint, and Excel, the actuator uses Microsoft's COM interface for automation.

• The script launch and file open activities run the script directly and open the file via start.exe respectively.

# CHANGE MANAGEMENT

When a Blue Team wants to make a change that materially affects configuration of a core system, they should follow the change management process and submit a change request. The change request should include the following elements:

* A detailed description of the process or configuration commands to achieve the change.
* Justification for the change
* Test Plan
  + Test(s) to validate change was effective (i.e. met the stated objectives for the change).
  + Test(s) to validate the change did not cause any adverse network impact. These tests will validate that the requested change has not broken or negatively impacted required network services.
* The Rollback Plan. The detailed process and/or configuration commands that will be used to remove the change and restore the network/device(s) to the previously unmodified state.



**Change Management Process**

