Current Scenarios & Environments

ThreatGEN® Red vs. Blue - Tabletop Exercise (TTX) Module

Scenarios

Scenarios currently available, with additional scenarios available later this fourth quarter 2022:

1) **Targeting your profit & loss** – The adversary is focused on dropping your profit & loss by any means necessary.
2) **Social engineering as an attack vector (easy)** – The adversary will deploy all forms of social engineering attacks, campaigns, and malicious USB drops as an initial attack vector.
3) **Social engineering as an attack vector (hard)** – The adversary will deploy all forms of social engineering attacks, campaigns and malicious USB drops as an initial attack vector. This adds more difficulty by lowering the initial security posture and giving the threat actor additional initial research.
4) **Physical security breach (easy)** – The adversary's only initial access vector is physical access.
5) **Physical security breach (hard)** – The adversary's only initial access vector is physical access. This adds more difficulty by lowering the initial security posture and giving the threat actor additional initial research.
6) **Classic cyber-attack scenario (easy)** – The adversary focuses solely on direct cyber-attacks. Little to no physical access or social engineering.
7) **Classic cyber-attack scenario (hard)** – The adversary focuses solely on direct cyber-attacks. Little to no physical access or social engineering. This adds more difficulty by lowering the initial security posture and giving the threat actor additional initial research.
8) **E-mail phishing attacks (easy)** – The adversary will use e-mail phishing campaigns and spear phishing as an initial attack vector.
9) **E-mail phishing attacks (hard)** – The adversary will use e-mail phishing campaigns and spear phishing as an initial attack vector. This adds more difficulty by lowering the initial security posture and giving the threat actor additional initial research.
10) **Blackmatter Ransomware** – Blackmatter ransomware threat actors have attacked numerous U.S.-based organizations and have demanded ransom payments, exfiltrated data for extortion and wiped backup systems.
11) **Ransomware threat actor (easy)** – The adversary will use spear phishing as an initial attack vector and then deploy ransomware on as many assets as it can while moving laterally.
12) **Ransomware threat actor (hard)** – The adversary will use spear phishing as an initial attack vector and then deploy ransomware on as many assets as it can while moving laterally. This adds more difficulty by lowering the initial security posture and giving the threat actor additional initial research.

New scenarios are added at least quarterly reflecting current threat actors and campaigns, keeping your staff trained to defend against the latest threats emerging onto the threat landscape.

Network Environments

Network environments (sometimes referred to as "*levels*" or "*maps*") currently available within the platform, with additional network environments available later in fourth quarter 2022:

- **Pipeline Company** – The pipeline company is a medium sized environment with industrial control systems (ICS) in the form of a supervisory control and data acquisition (SCADA) system as well as a distributed control system (DCS).
- **Manufacturing Plant** – The manufacturing plant is a small environment with industrial control systems (ICS) in the form of a single distributed control system (DCS).
- **Large Oil & Gas Company** – The large oil & gas company is a large environment with industrial control systems (ICS) in the form of a supervisory control and data acquisition (SCADA) system as well a distributed control system (DCS).
- **IT Services Company** – The IT Services company is a small IT environment with a focus on providing external helpdesk / technical support capabilities.
- **G.R.E.G. Facility** – The Gas Resource Extraction Group Facility is a medium environment with industrial control systems (ICS) in the form of a single distributed control system (DCS).
- **Software Development Company** – The IT service company is a medium IT environment with a focus on software development.
- **CDN Point of Presence Network** – The CDN Point of Presence Network is a medium IT environment providing content delivery services.
- **Large Legal Office** – The Large Legal Office is a large IT environment with a focus on providing legal services.
- **Data Science Company** – The Data Science Company is a small IT environment with a focus on large data analysis.
- **Marketing Company** – The Marketing Company is a large IT environment with a focus on providing marketing services.
- **Printing Company** – The Printing Company is a small environment with industrial control systems (ICS) in the form of a single distributed control system (DCS).
- **Car Manufacturing Facility** – The Car Manufacturing Facility is a large environment with industrial control systems (ICS) in the form of a supervisory control and data acquisition (SCADA) system as well as a distributed control system (DCS).
- **The Casino** – The Casino is a medium IT environment with a focus on gambling and entertainment services.
- **Railway System** – The Railway System is a large environment with industrial control systems (ICS) in the form of a supervisory control and data acquisition (SCADA) system as well as a distributed control system (DCS).