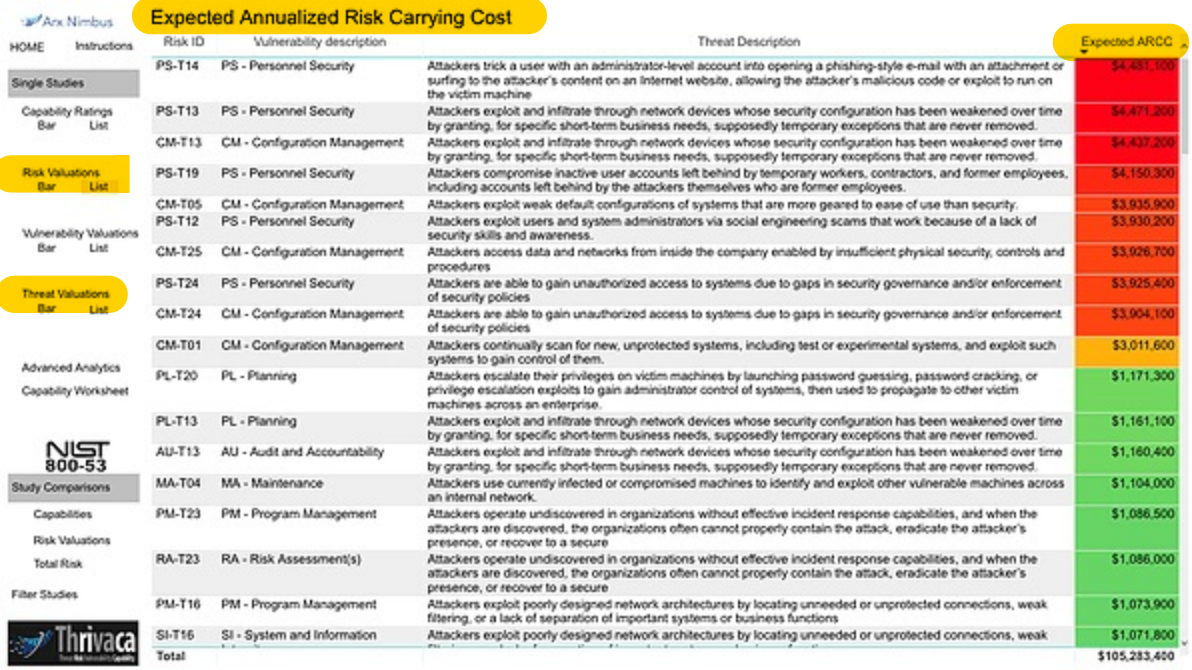
Ark Nimbus
HOME
Instructions
Single Studies
Capability Ratings
Bar
List
Risk Valuations
Bar
List
Vulnerability Valuations
Bar
List
Threat Valuations
Bar
List
Advanced Analytics
Capability Worksheet
NIST 800-53
Study Comparisons
Capabilities
Risk Valuations
Total Risk
Filter Studies
Thrivaca
Expected Annualized Risk Carrying Cost
Risk ID
Vulnerability description
Threat Description
Expected ARCC
PS-T14
PS - Personnel Security
Attackers trick a user with an administrator-level account into opening a phishing-style e-mail with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine
$4,481,100
PS-T13
PS - Personnel Security
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.
$4,471,200
CM-T13
CM - Configuration Management
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.
$4,437,200
PS-T19
PS - Personnel Security
Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees.
$4,150,300
CM-T05
CM - Configuration Management
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.
$3,935,900
PS-T12
PS - Personnel Security
Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness.
$3,930,200
CM-T25
CM - Configuration Management
Attackers access data and networks from inside the company enabled by insufficient physical security, controls and procedures
$3,926,700
PS-T24
PS - Personnel Security
Attackers are able to gain unauthorized access to systems due to gaps in security governance and/or enforcement of security policies
$3,925,400
CM-T24
CM - Configuration Management
Attackers are able to gain unauthorized access to systems due to gaps in security governance and/or enforcement of security policies
$3,904,100
CM-T01
CM - Configuration Management
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.
$3,011,600
PL-T20
PL - Planning
Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, then used to propagate to other victim machines across an enterprise.
$1,171,300
PL-T13
PL - Planning
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.
$1,161,100
AU-T13
AU - Audit and Accountability
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.
$1,160,400
MA-T04
MA - Maintenance
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.
$1,104,000
PM-T23
PM - Program Management
Attackers operate undiscovered in organizations without effective incident response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure
$1,086,500
RA-T23
RA - Risk Assessment(s)
Attackers operate undiscovered in organizations without effective incident response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure
$1,086,000
PM-T16
PM - Program Management
Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions
$1,073,900
SI-T16
SI - System and Information
Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak
$1,071,800
Total
$105,283,400