Distributed Vulnerability Assessment

Information security is not an objective property of information …

Information security is not an objective property of information …

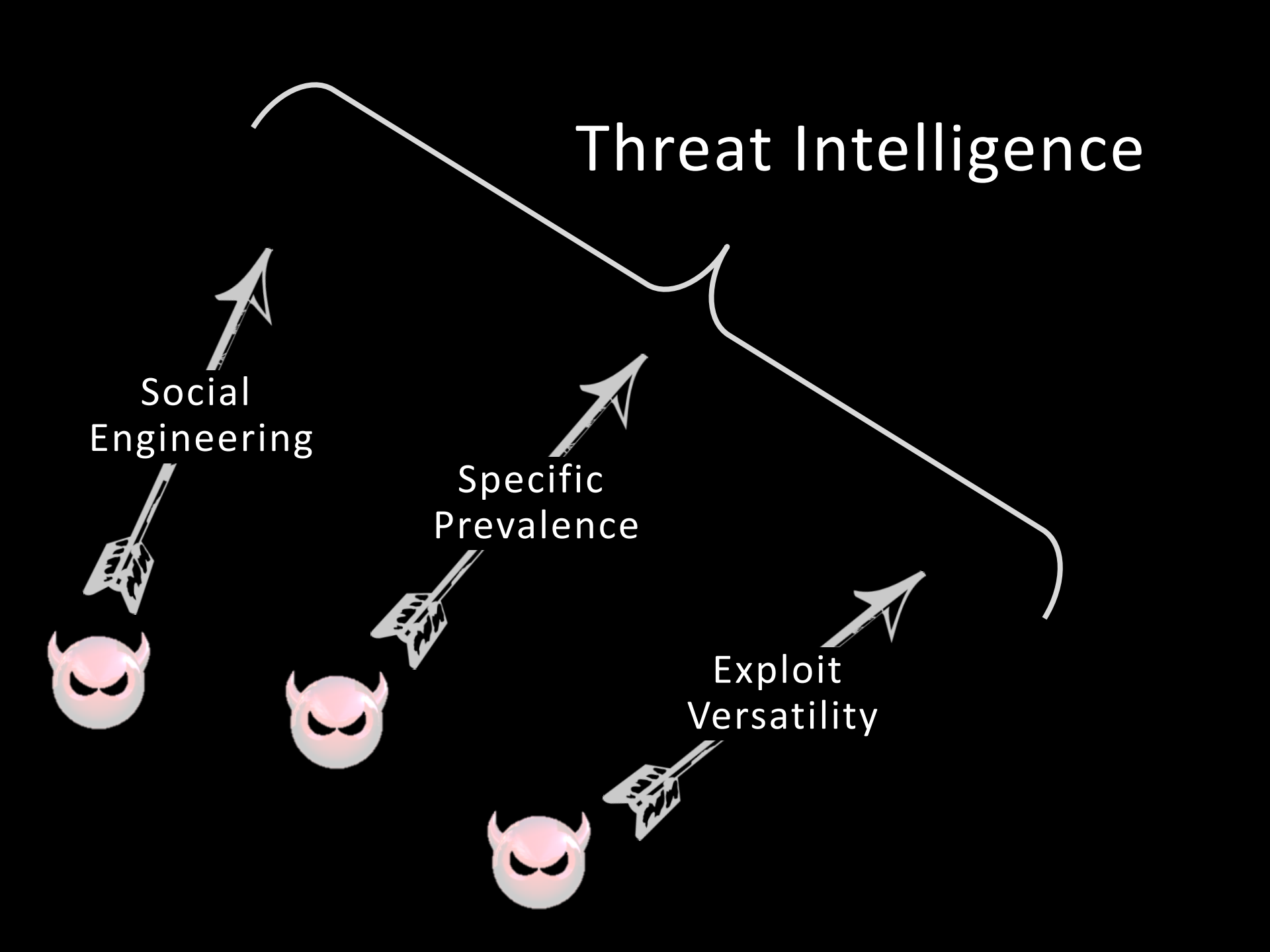
… rather it is a subjective service for people who use information.

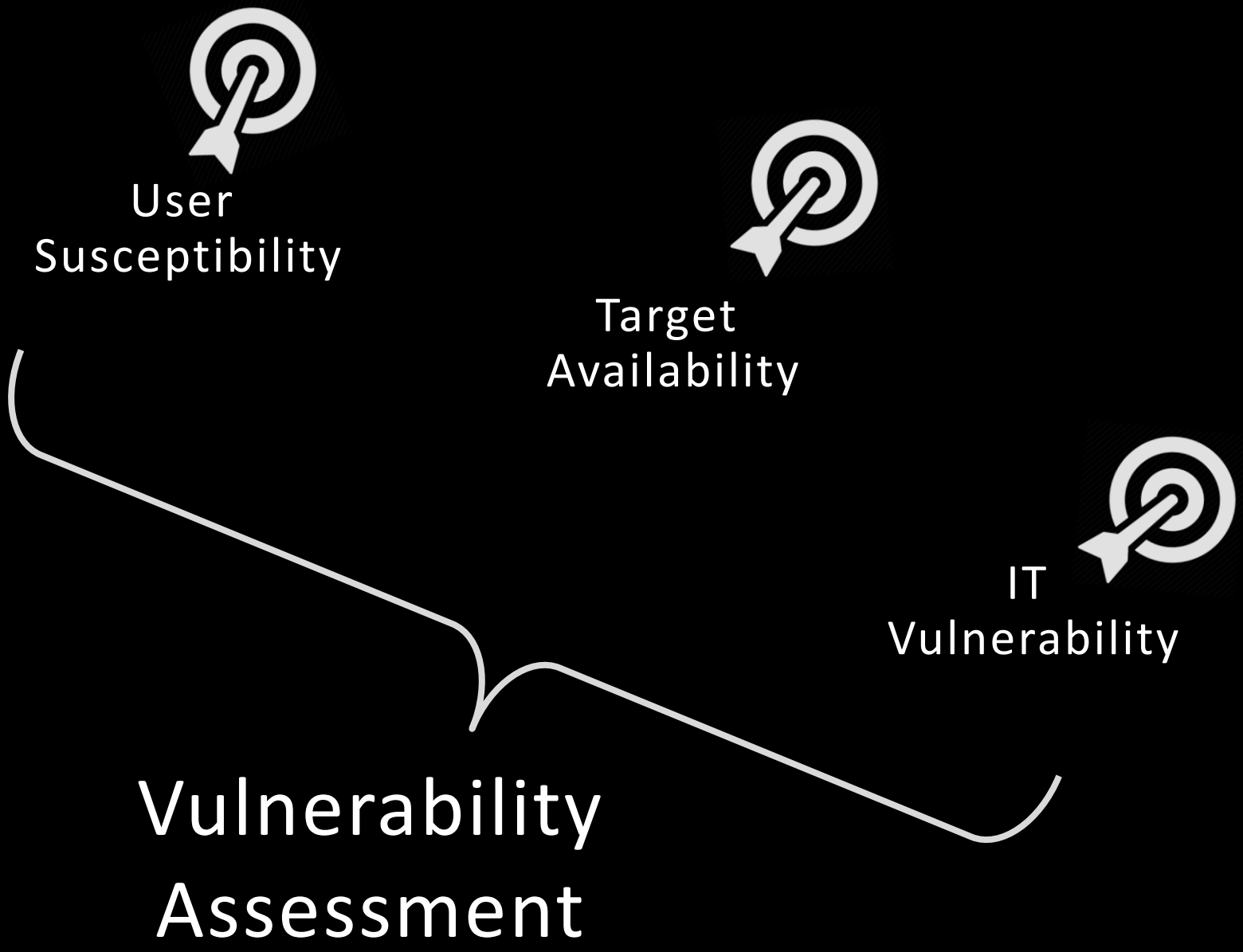
Relative Known Threats

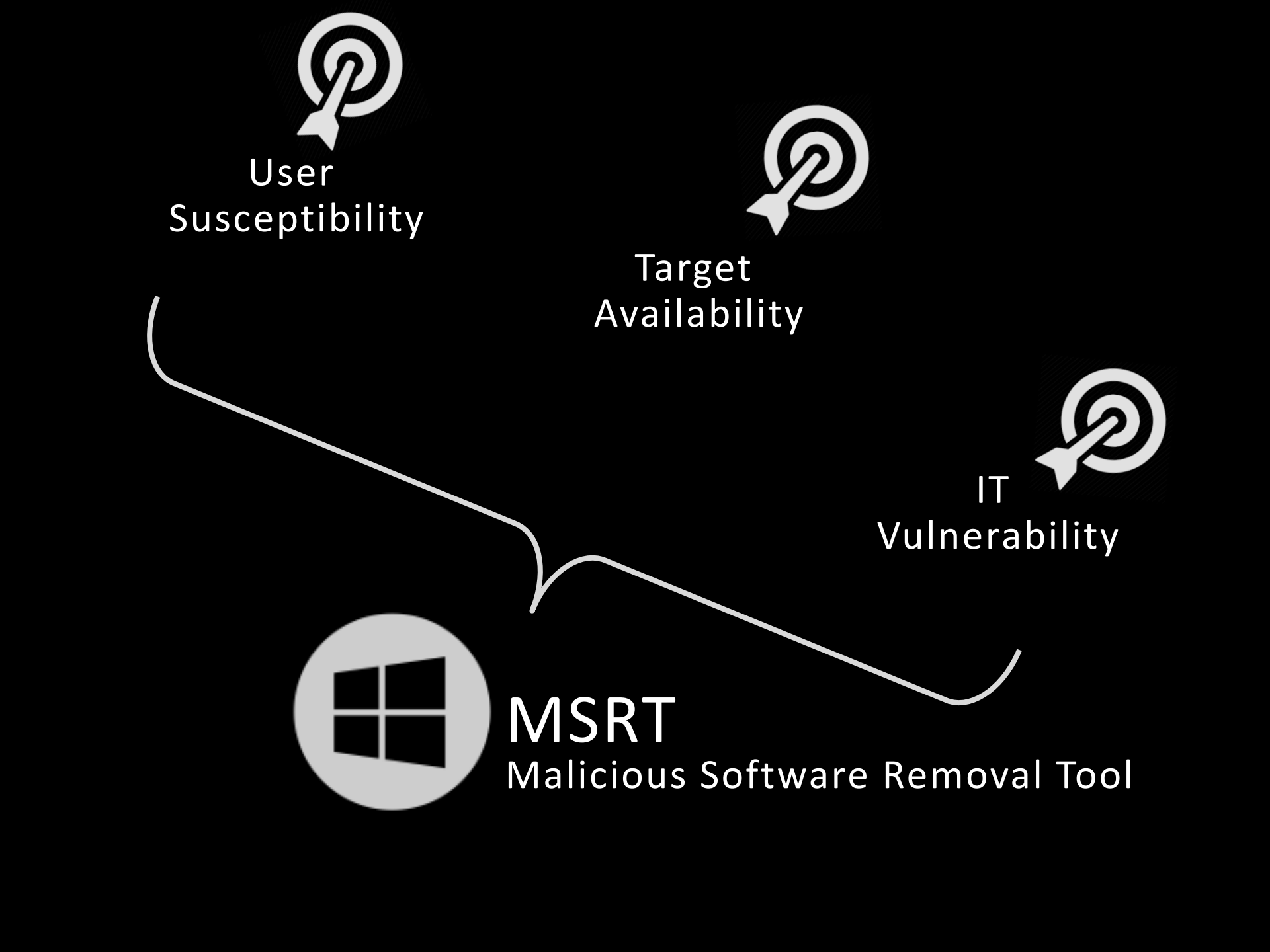
Properties of Malware

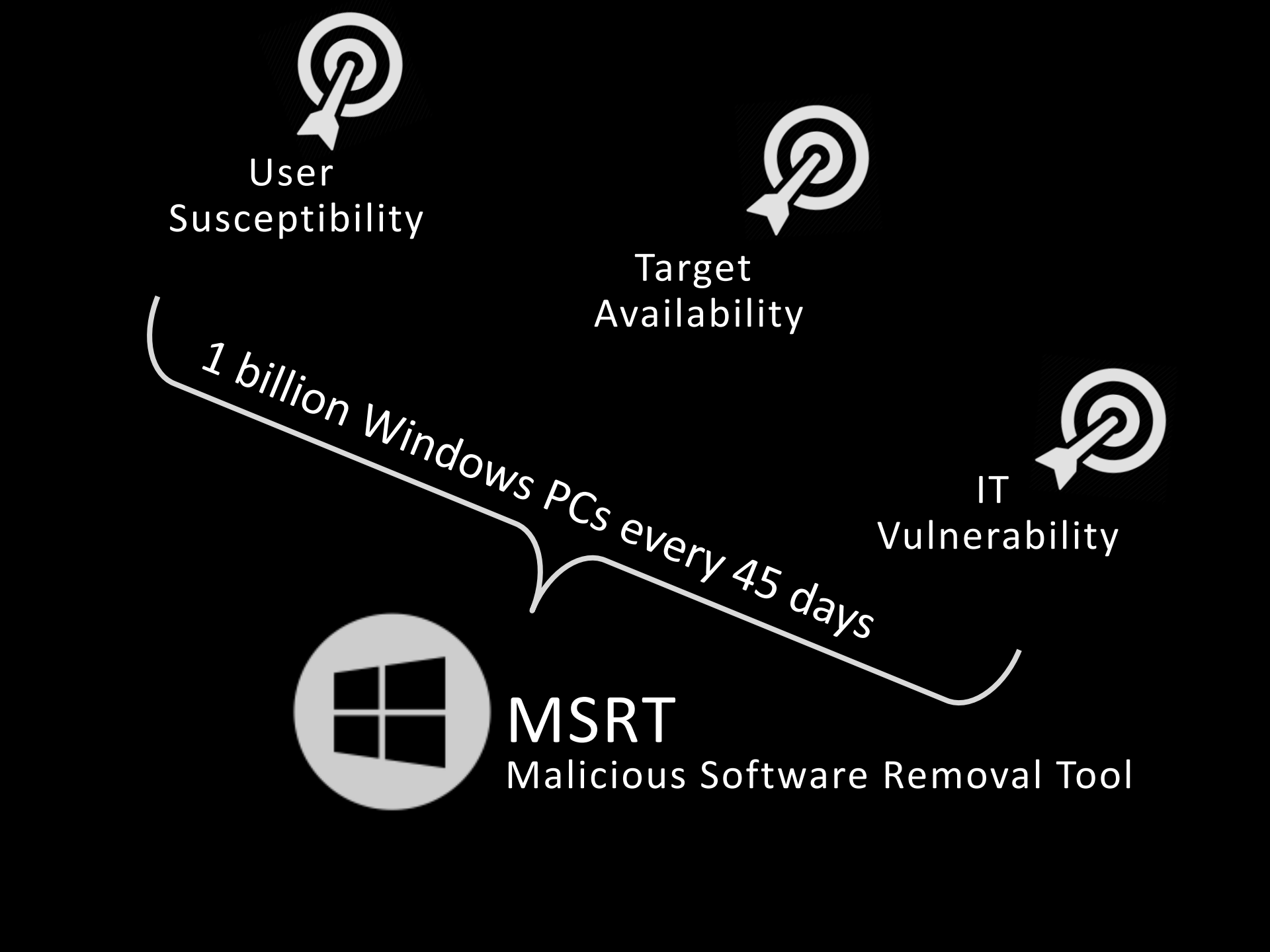
Relative Known Vulnerabilities

Properties of the Enterprise


Threat Intelligence
Social Engineering
Specific Prevalence
Exploit Versatility


User
Susceptibility
Target
Availability
IT
Vulnerability
Vulnerability
Assessment


User
Susceptibility
Target
Availability
IT
Vulnerability
MSRT
Malicious Software Removal Tool


User
Susceptibility
Target
Availability
IT
Vulnerability
1 billion Windows PCs every 45 days
MSRT
Malicious Software Removal Tool

Software programs
(like machine parts)
are instances of some functionality …

Software programs
(like machine parts)
are instances of some functionality …

… IT endpoints
(like people)
are uniquely themselves

Because,
at the end of each point,
there is always a person

(or maybe the IoT agent of a person)

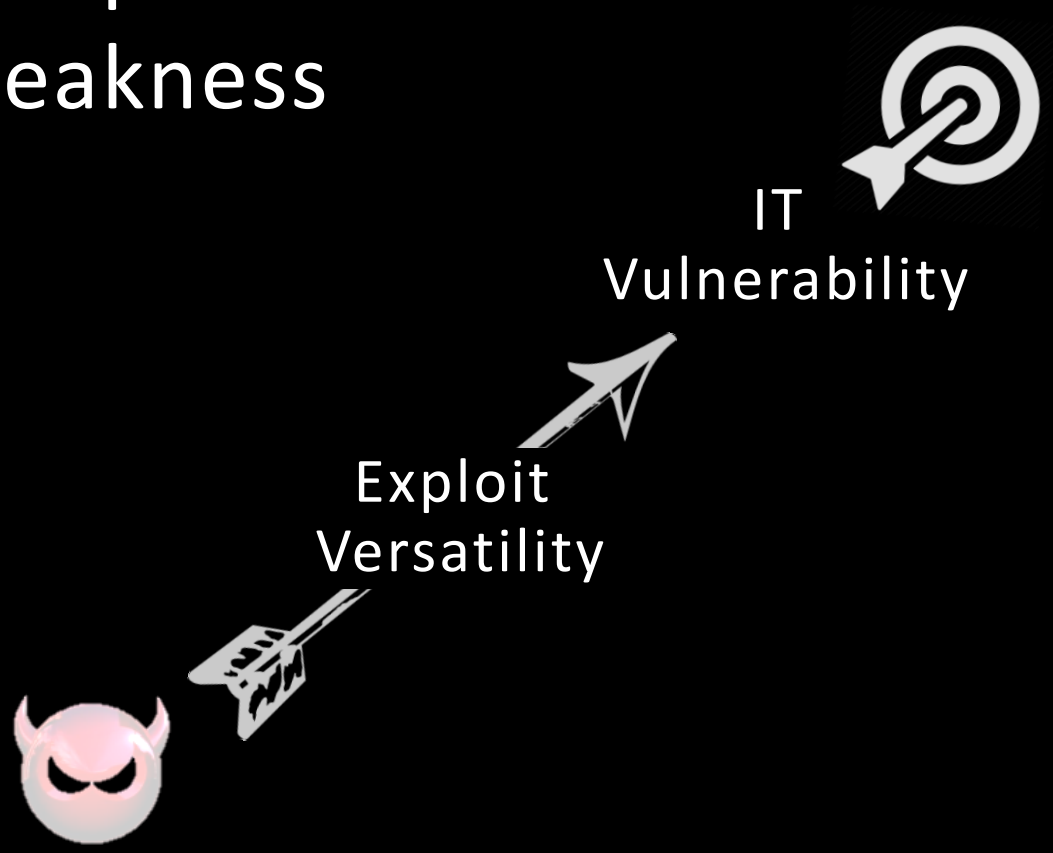
Because,
at the end of each point,
there is always a person
(or maybe the IoT agent of a person)

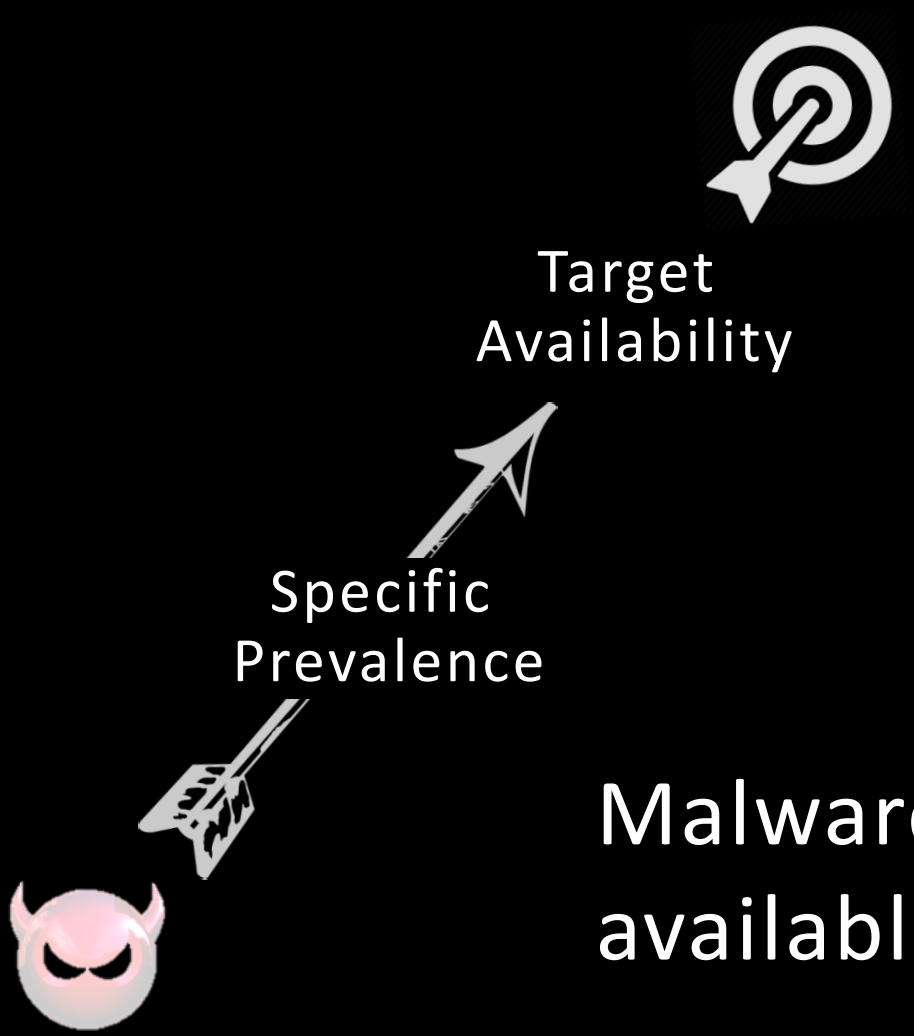
And people are never interchangeable

How interchangeable are endpoints ?

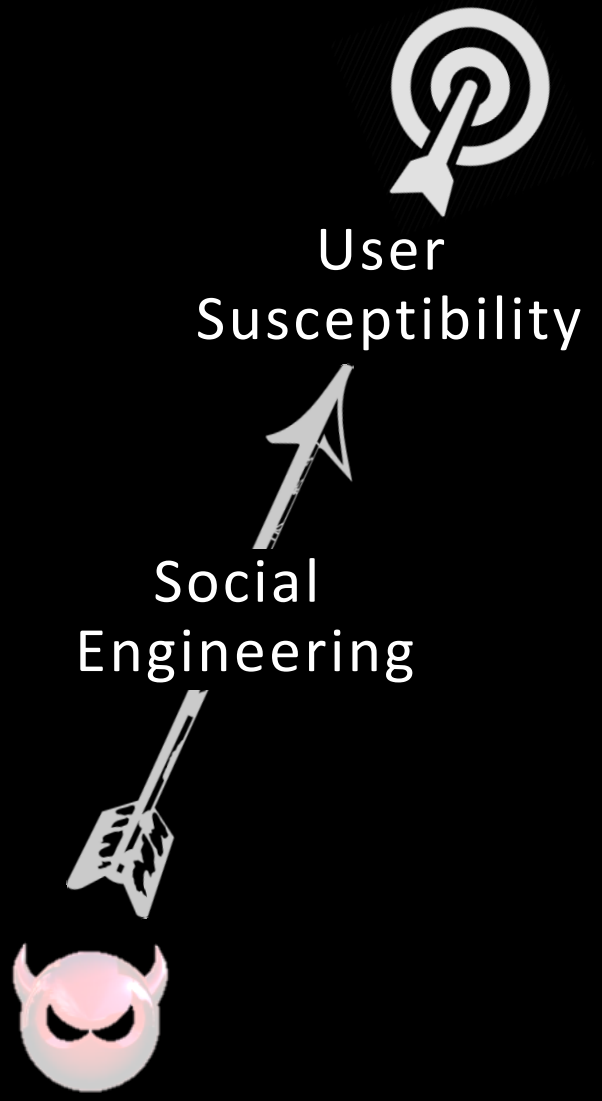
Source: https://www.youtube.com/watch?v=AkoML0_FiV4

Malware exploits technical weakness

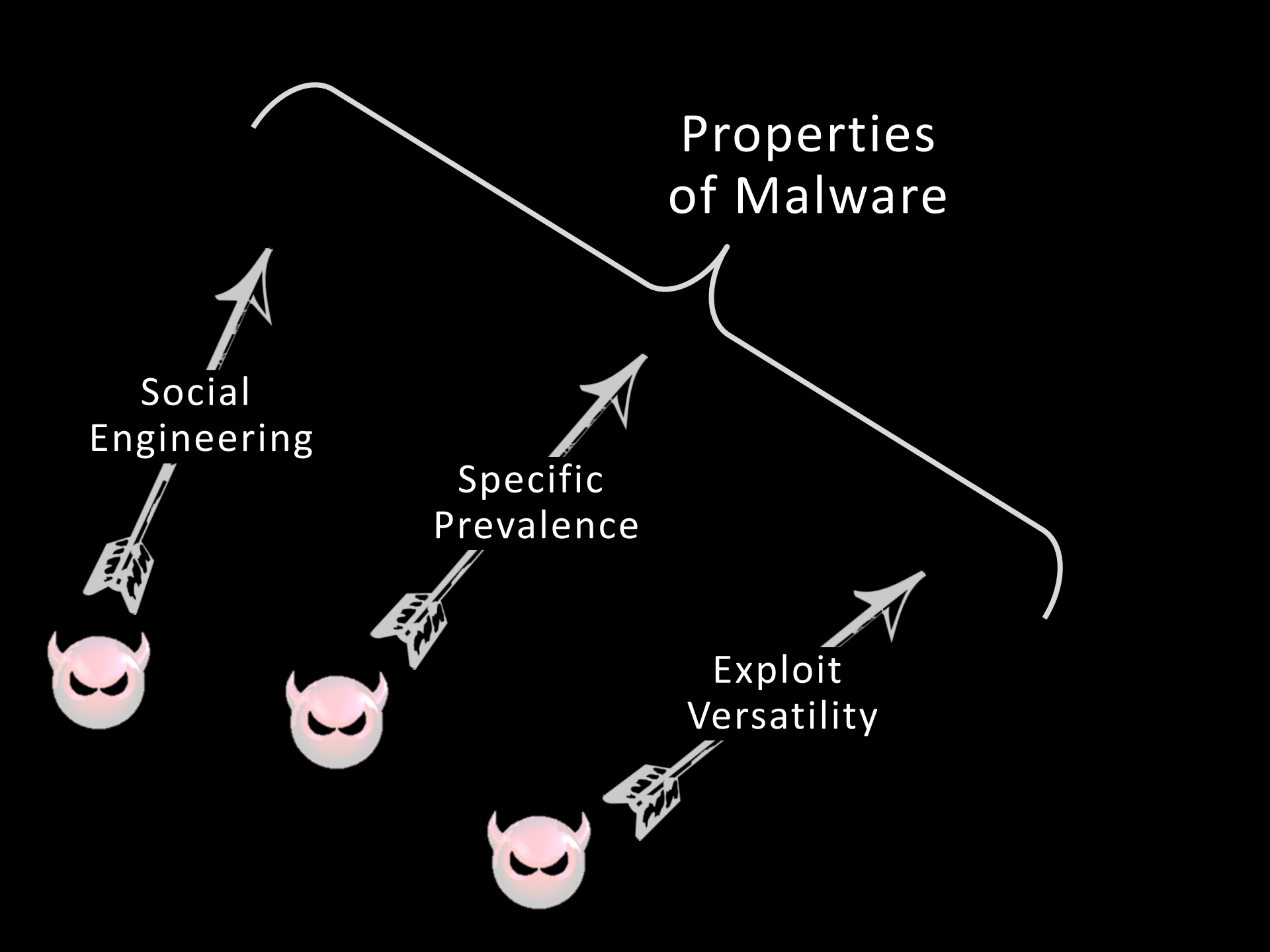


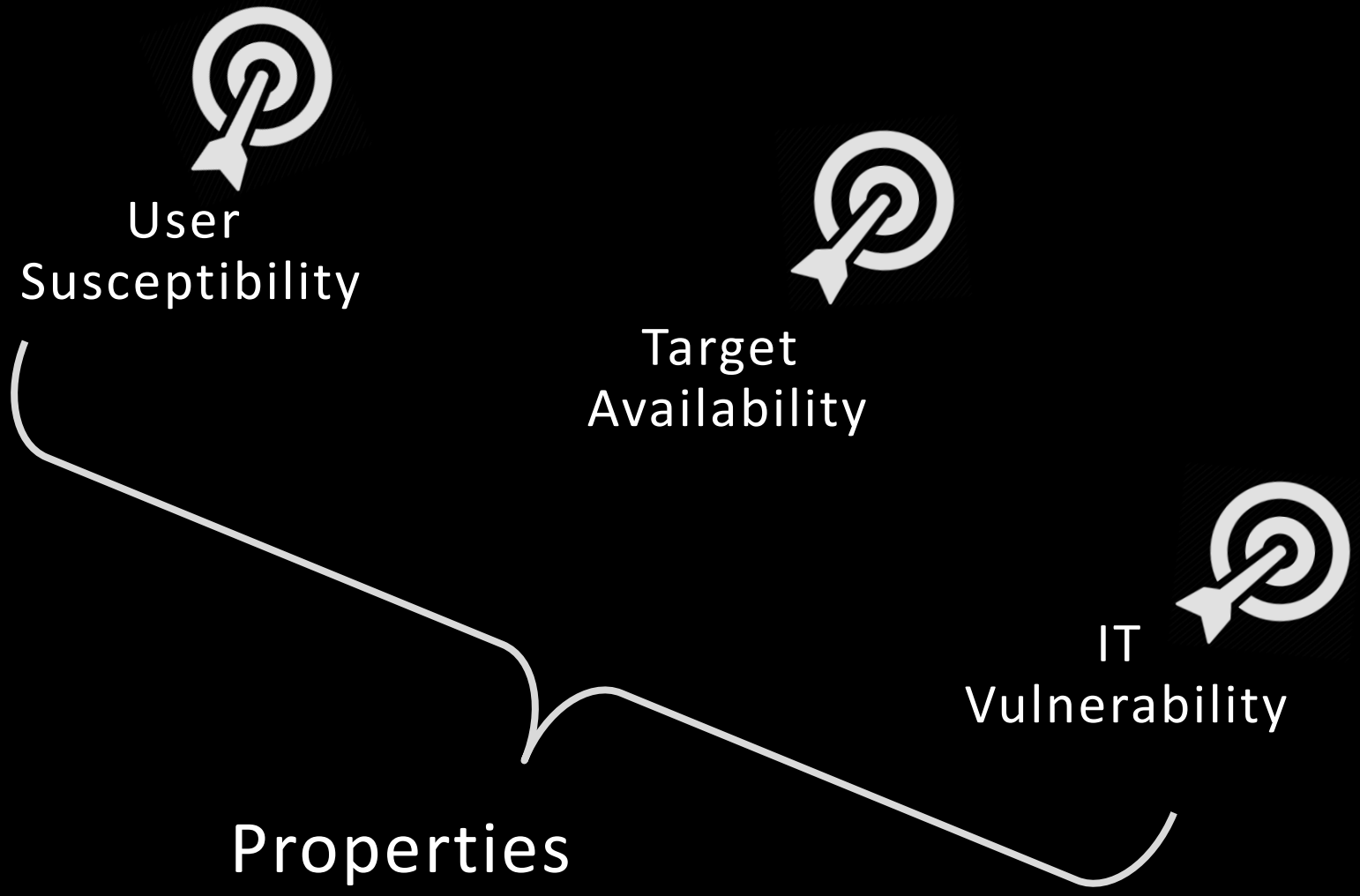


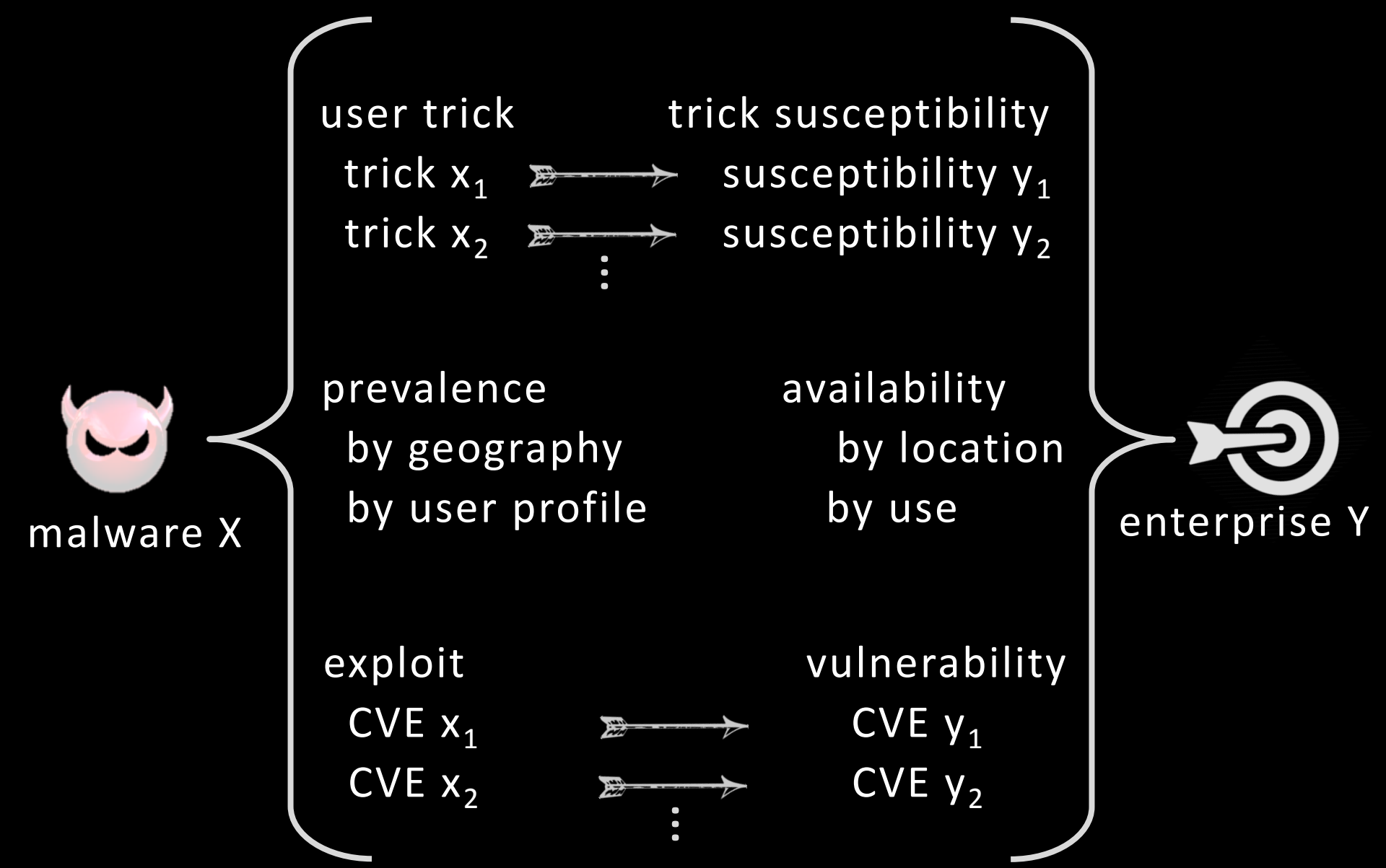
Malware thrives on available targets



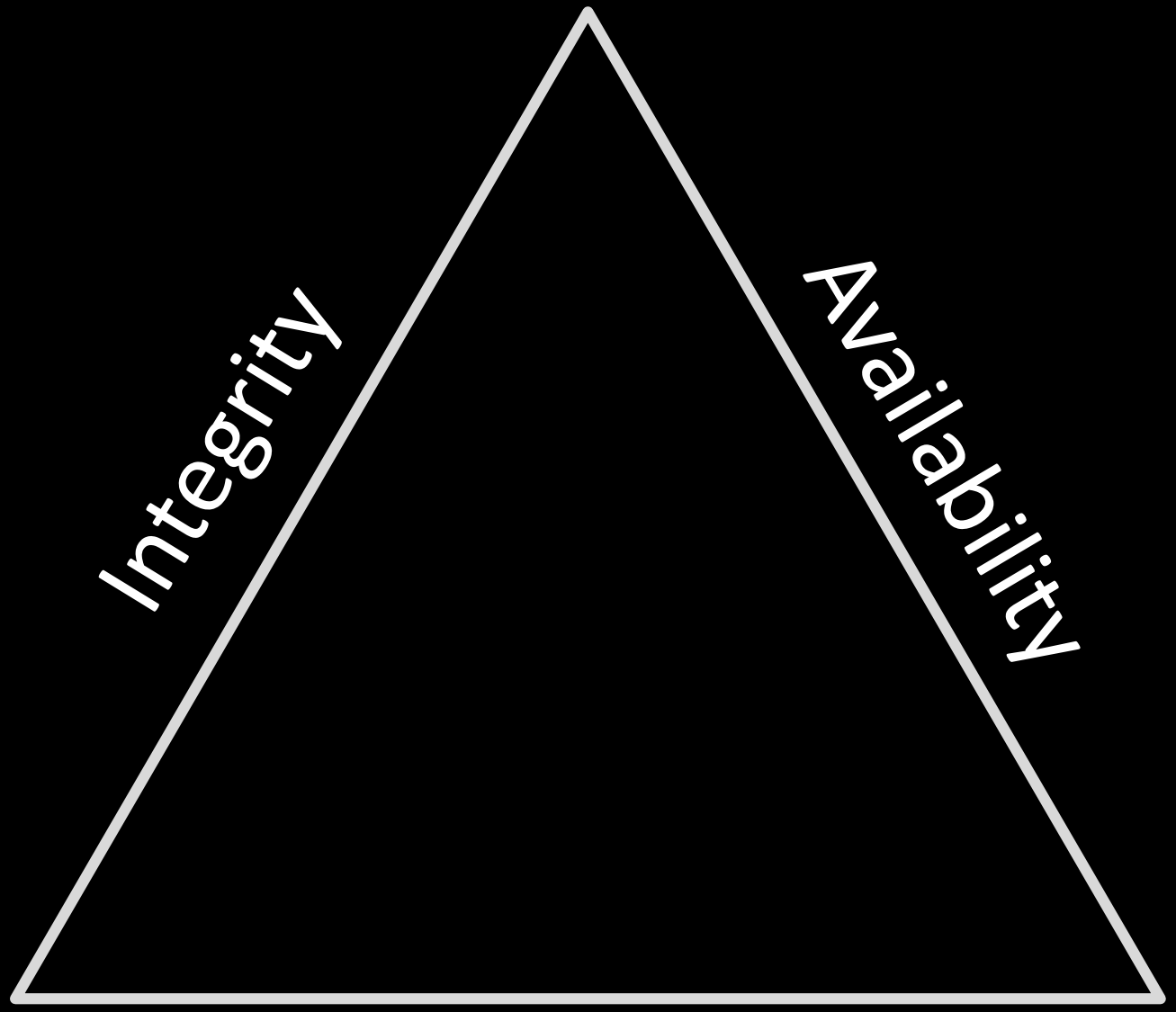
Malware manipulates human agents

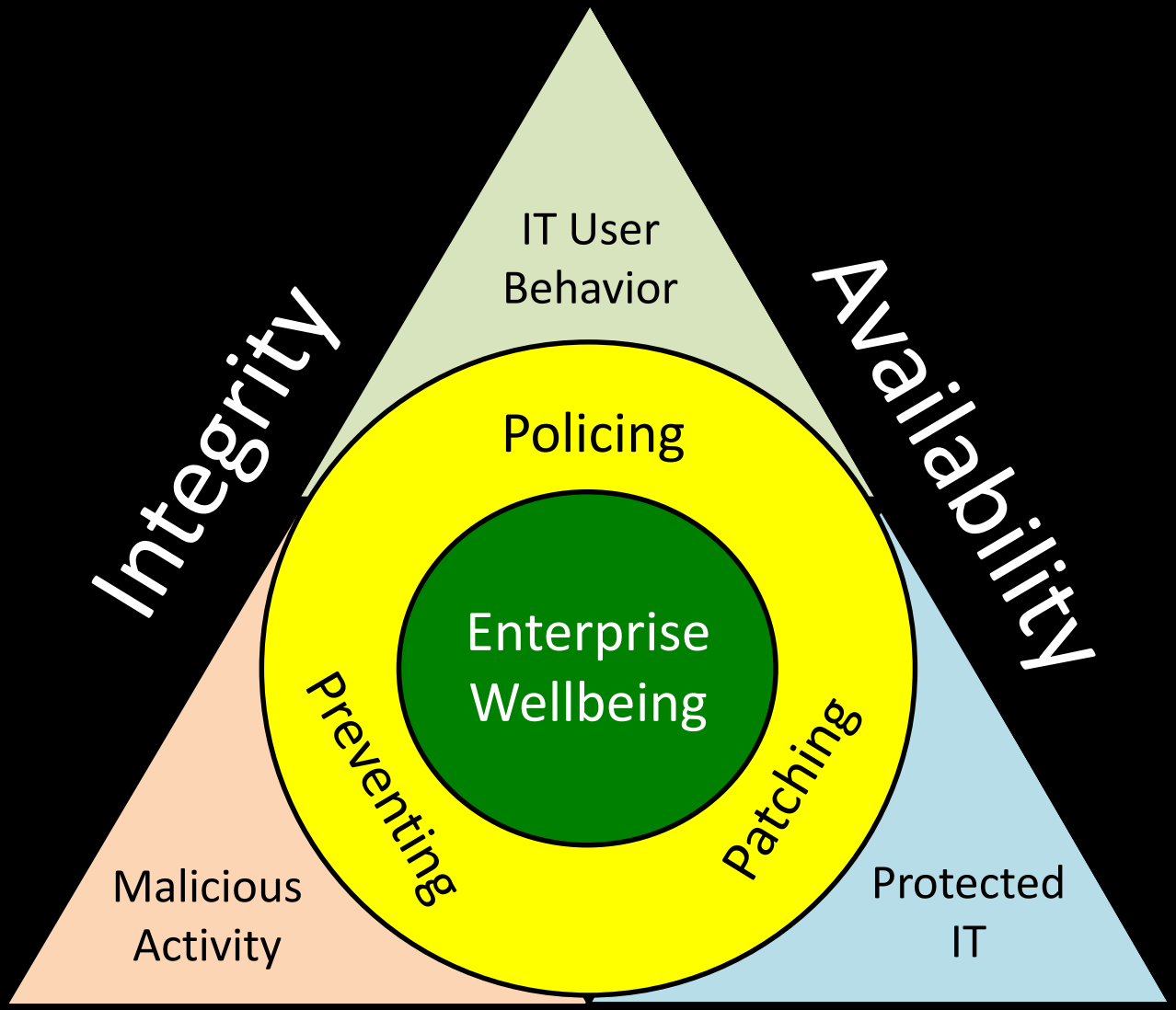

Properties
of Malware
Social
Engineering
Specific
Prevalence
Exploit
Versatility


User
Susceptibility
Target
Availability
IT
Vulnerability
Properties
of Enterprises



Assessed separately for each threat at each enterprise


Integrity
Availability
Confidentiality

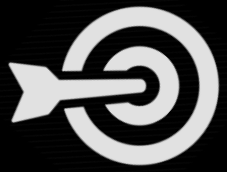

IT User Behavior
Integrity
Availability
Policing
Enterprise Wellbeing
Preventing
Patching
Malicious Activity
Protected IT
Confidentiality

malware X

Specific vulnerability of enterprise Y to malware threat X

50

enterprise Y



Relative vulnerability contribution by source

M1, M2, …
U1, U2, …
I1, I2, …

Distributed Vulnerability Assessment

Distributed Vulnerability Assessment