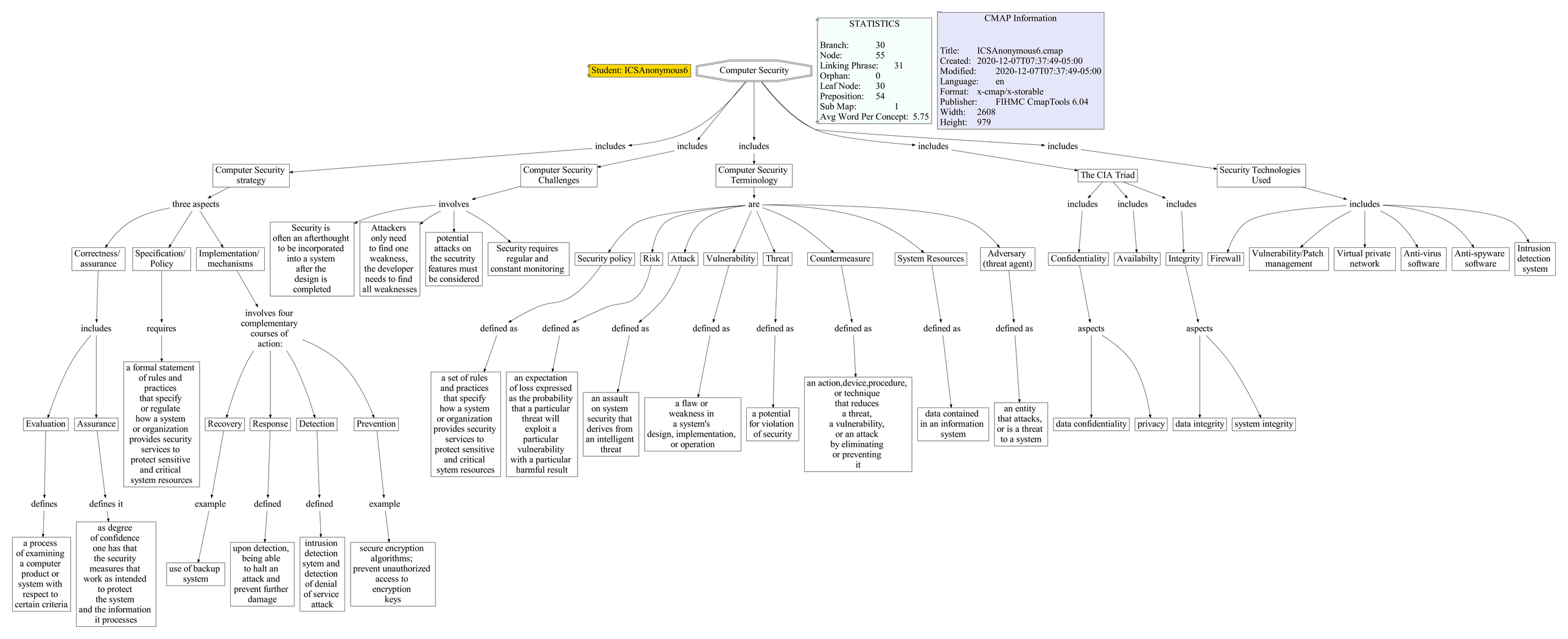
Student: ICSAnonymous6
Computer Security
STATISTICS
Branch: 30
Node: 55
Linking Phrase: 31
Orphan: 0
Leaf Node: 30
Preposition: 54
Sub Map: 1
Avg Word Per Concept: 5.75
CMAP Information
Title: ICSAnonymous6.cmap
Created: 2020-12-07T07:37:49-05:00
Modified: 2020-12-07T07:37:49-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 2608
Height: 979
includes
includes
includes
includes
includes
Computer Security strategy
Computer Security Challenges
Computer Security Terminology
The CIA Triad
Security Technologies Used
three aspects
involves
are
includes
includes
includes
includes
Correctness/ assurance
Specification/ Policy
Implementation/ mechanisms
Security is often an afterthought to be incorporated into a system after the design is completed
Attackers only need to find one weakness, the developer needs to find all weaknesses
potential attacks on the securtity features must be considered
Security requires regular and constant monitoring
Security policy
Risk
Attack
Vulnerability
Threat
Countermeasure
System Resources
Adversary (threat agent)
Confidentiality
Availabilty
Integrity
Firewall
Vulnerability/Patch management
Virtual private network
Anti-virus software
Anti-spyware software
Intrusion detection system
includes
requires
involves four complementary courses of action:
defined as
defined as
defined as
defined as
defined as
defined as
defined as
defined as
aspects
aspects
Evaluation
Assurance
a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
Recovery
Response
Detection
Prevention
a set of rules and practices that specify how a system or organization provides security services to protect sensitive and critical sytem resources
an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result
an assault on system security that derives from an intelligent threat
a flaw or weakness in a system's design, implementation, or operation
a potential for violation of security
an action,device,procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it
data contained in an information system
an entity that attacks, or is a threat to a system
data confidentiality
privacy
data integrity
system integrity
defines
defines it
example
defined
defined
example
a process of examining a computer product or system with respect to certain criteria
as degree of confidence one has that the security measures that work as intended to protect the system and the information it processes
use of backup system
upon detection, being able to halt an attack and prevent further damage
intrusion detection sytem and detection of denial of service attack
secure encryption algorithms; prevent unauthorized access to encryption keys