Notes

The Cisco Security Ninja program is a technical security awareness program created in 2012. The goal of this program is to change the security culture of Cisco from within.

This slide deck is an example of a module that exists within our first level, White Belt. The purpose of this deck is to highlight our content style, and allow others to see what we do, and learn from it.

We use graphics throughout because we take pride in our offering, and we want it to be the best possible content and visual experience for the learner. Graphics convey concepts better than words, and we employ them for teaching, not just for looks.

Notes

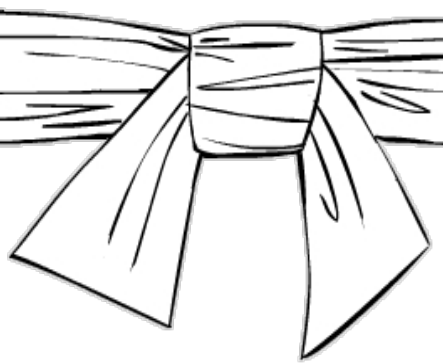
Video is our primary delivery mechanism, with slides being used to drive the conversation. We do not read from the slides EVER. Our format is more like a security talk show then a presentation. We are not afraid to joke or laugh in the middle of a module. We include real subject matter experts from across Cisco to help us teach.

Cisco Security Ninja Training

Sample Module

Authored by: Chris Romeo

Notes

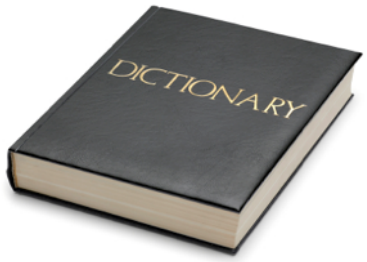


Learning outcomes introduce the learner to what we intend to teach on a high level. This prepares them, and introduces the concepts that we will dive deeper into within the module.

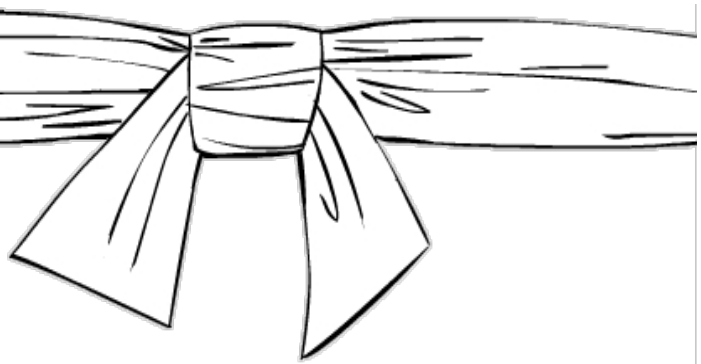
Learning Outcomes

By the end of this module, you will be able to:

- ✓ Model key term understanding and usage
- ✓ Define core security terms
- ✓ Recognize threats, vulnerabilities, attacks and exploits



Notes

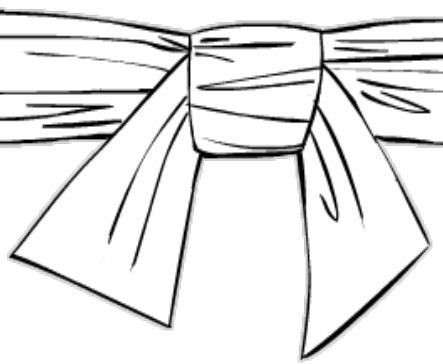


We like to include a “Why do you care?” slide because we know that many people that watch a module may not initially be excited about the content. Our “why you care” section sets the stage for the learner and connects the content to their world.

Why do YOU care?

- ✓ Basic understanding of security terms
- ✓ Communicate with a common language
- ✓ Terminology impacts thought and practice

Notes



We strive to use graphics to make complex topics more simple. The slides are used as a backdrop in our conversation. We try to create them to stand on their own, as some people like to just review slides.

Is it Secure? Consider C.I.A.

Information can only be **viewed by authorized** parties

Confidentiality

Of device, service, or data.

Integrity

Availability

Vulnerability

Vulnerability

A weakness, design or coding error, or lack of protection in a product that enables an attack

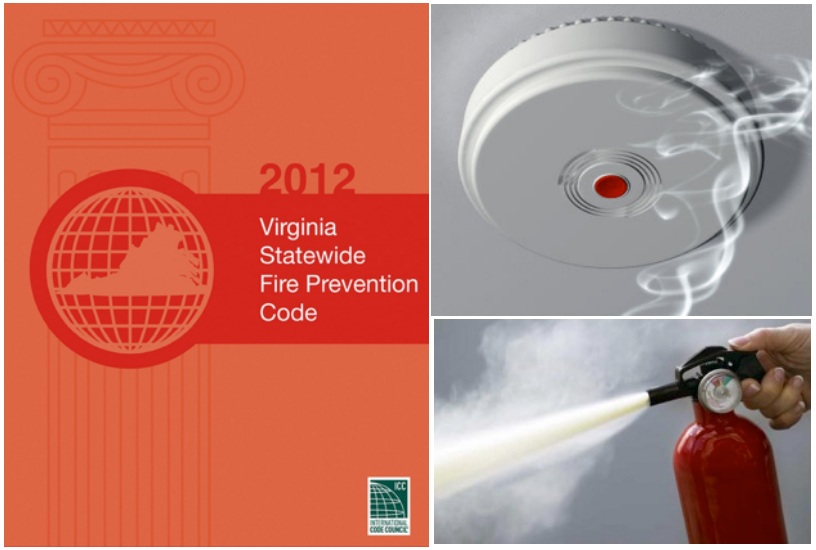
https://flic.kr/p/LhHyk

Vulnerabilities can result from Design, Programming, or Operational flaws.

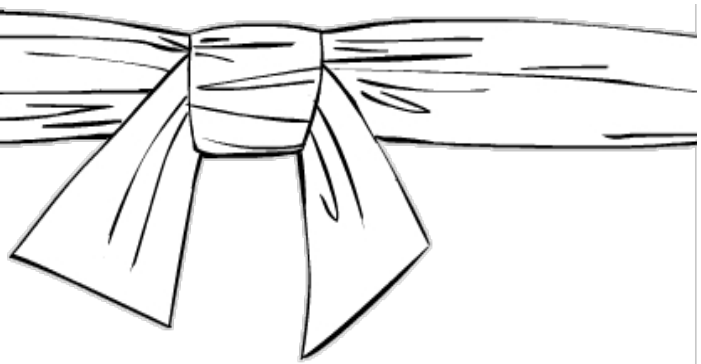
Mitigation

Mitigation

A strategy for reducing or eliminating the severity of a security issue



Notes



Key takeaways summarize the lessons imparted on the learner in this module. We follow the oldest strategy in the book, tell them what you will tell them, tell them, and tell them what you told them.

Key Take Aways

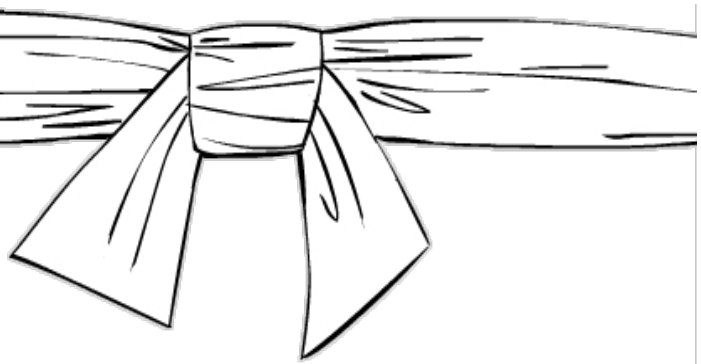
Important security characteristics and attack goals

- Confidentiality, Integrity and Availability
- Non-repudiation and Authenticity

Foundational Security Terms

- Threats, vulnerabilities, attacks and exploits
- Attack Surface!
- Exposures and their mitigations

Notes

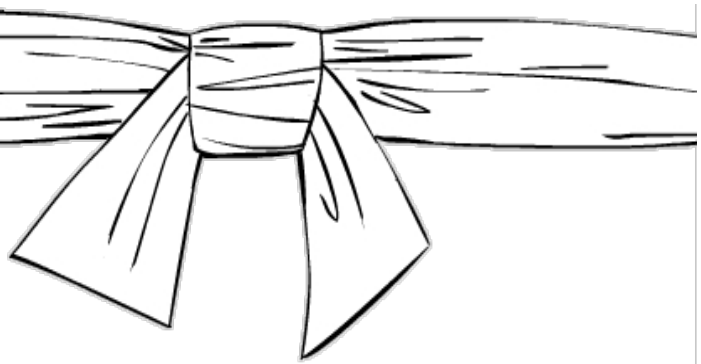


We store a resources slide that is never filmed. We use this slide to collect resources during the content development phase. Resources are added to a tab within our web interface, so a learner may dive deeper into any topic they choose.

Resources

Standard	Definition
CSDL	Cisco Secure Development Lifecycle -- A repeatable and measurable process designed to increase resiliency and trustworthiness of Cisco products
CAPEC	Common Attack Pattern Enumeration & Classification -- A publicly available, community-developed list of common attack patterns along with a comprehensive schema and classification taxonomy http://capec.mitre.org
OWASP	Open Web Application Security Project – san organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. http://www.owasp.org

Notes



We hope this overview of our learning approach for the Cisco Security White Belt has been helpful. It is our goal to share our approach with the community, to assist in building technical security awareness within all organizations.

If you have any questions, please contact me

Chris Romeo
chromeo@cisco.com
@edgeroute