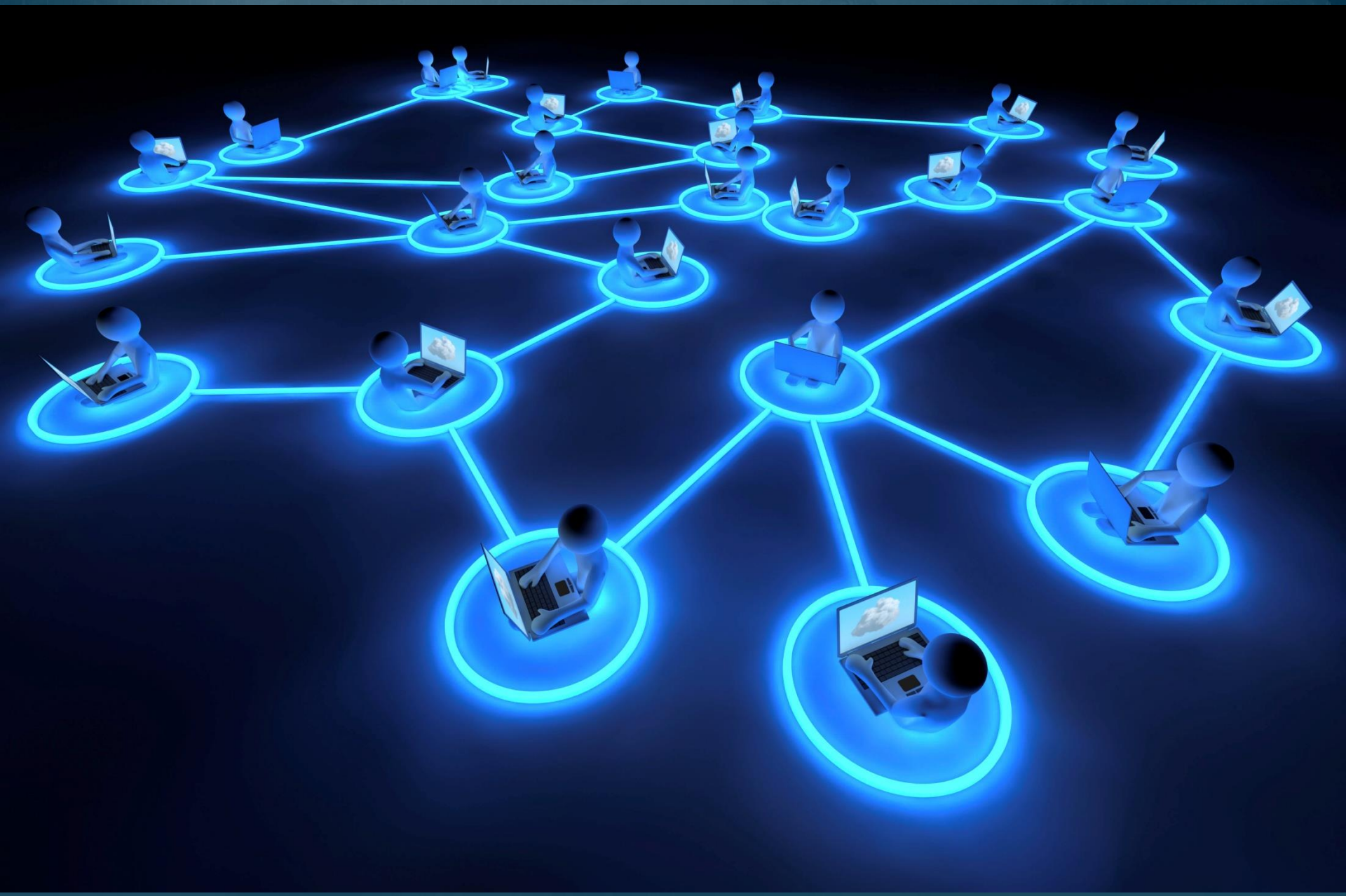
Evolving Security Automation Standards

CONFIDENCE IN CYBERSPACE

Presented by
Jessica Fitzgerald-McKay


spyware
spam
phishing
trojan
data security
virus
attack
malware
virus alert!
virus detected

CENTERS FOR DISEASE CONTROL AND PREVENTION



Security Automation – Knowing Your Network

CONFIDENCE IN CYBERSPACE

A Day in the Life of a Sysadmin

@%!#

Vulnerability Announcement

A Future Day in the Life of a Sysadmin

Router

Web Server

CA

Mac Endpoint

VPN Gateway

Domain Controllers

Linux Endpoint

Windows Endpoint

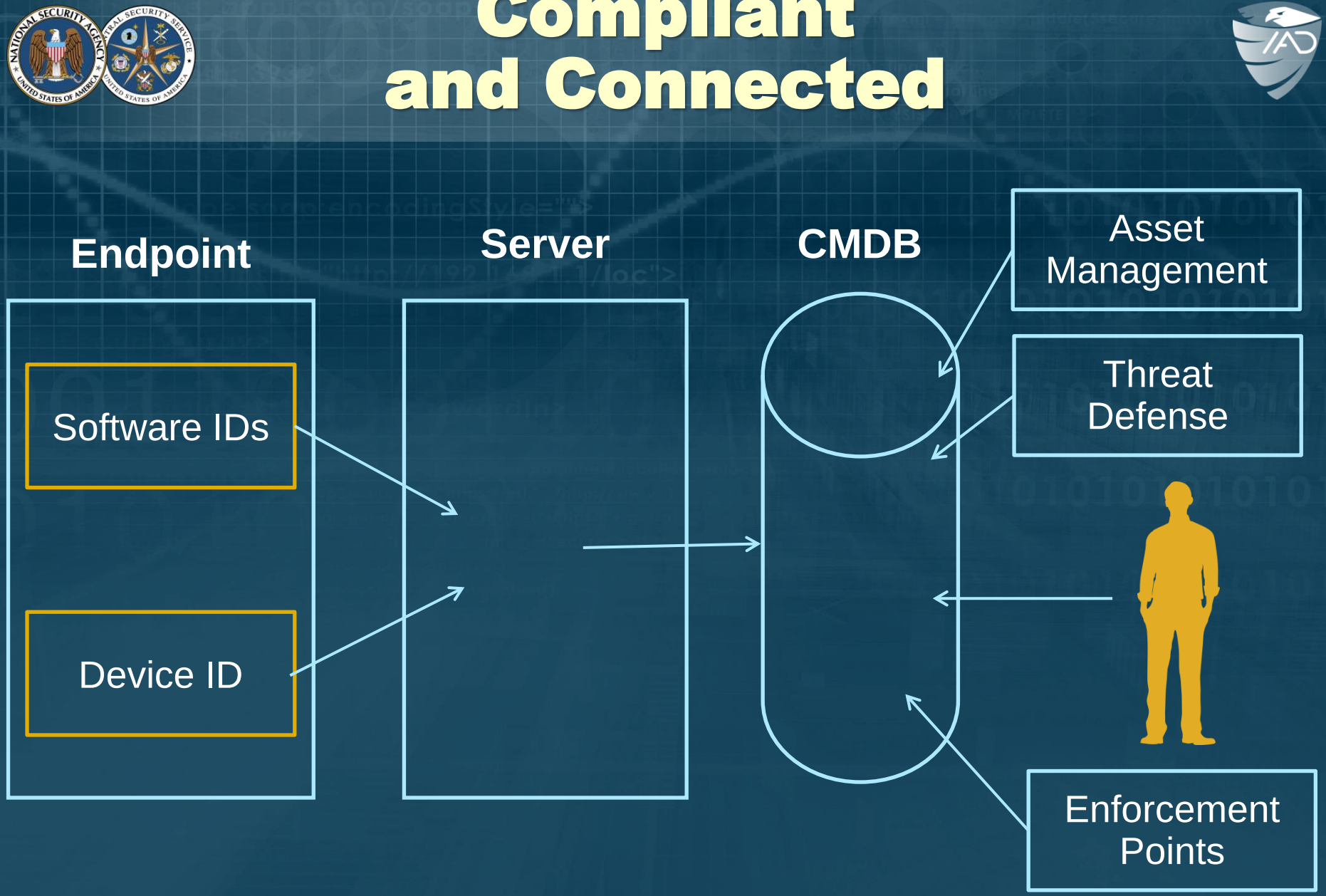
Knowing Your Network

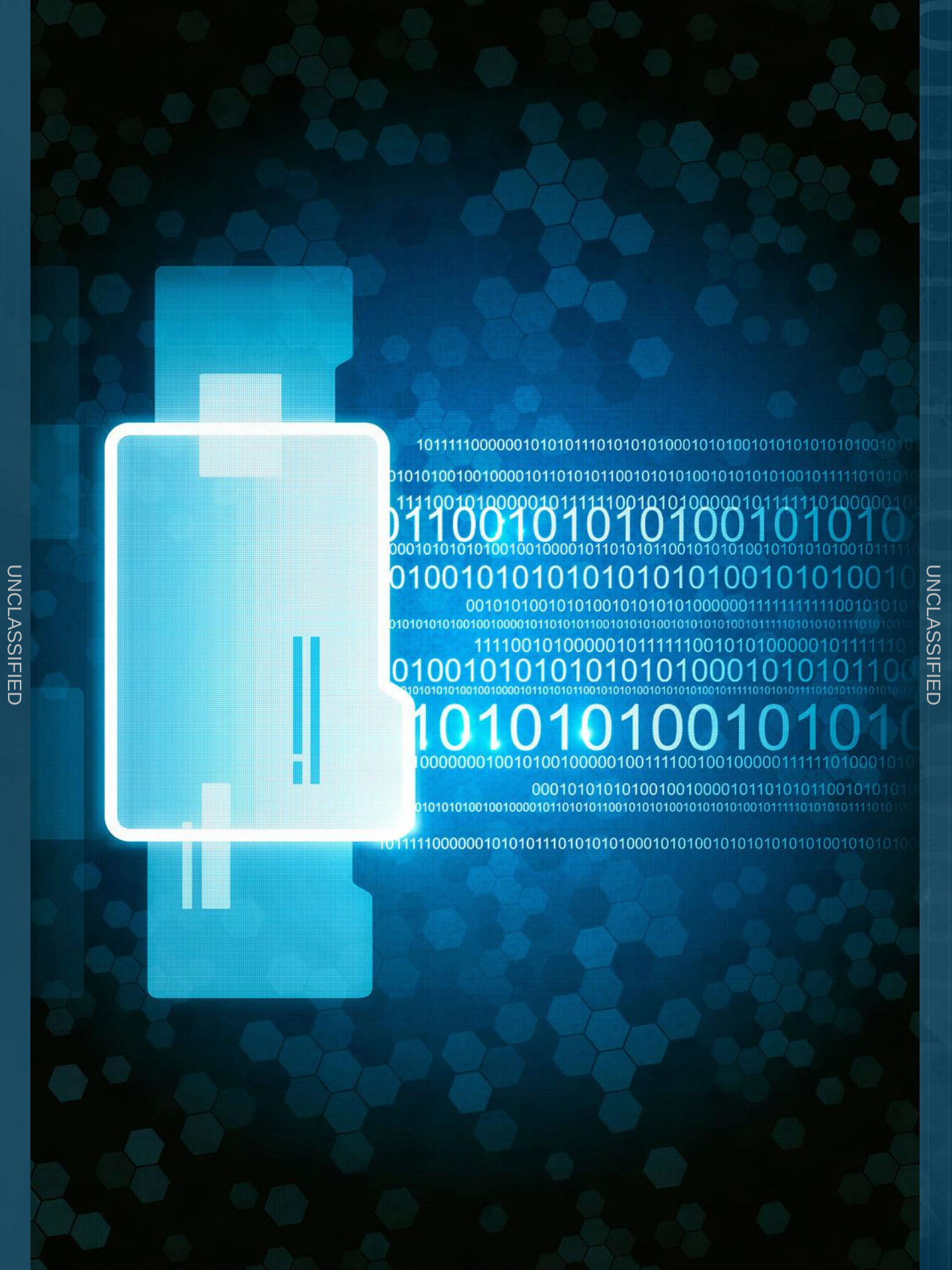
- **Need to know**
  - What is connected?
  - Is it authorized to be there?
  - Is it healthy?
  - Is it vulnerable?

Software Identification (SWID) Tags

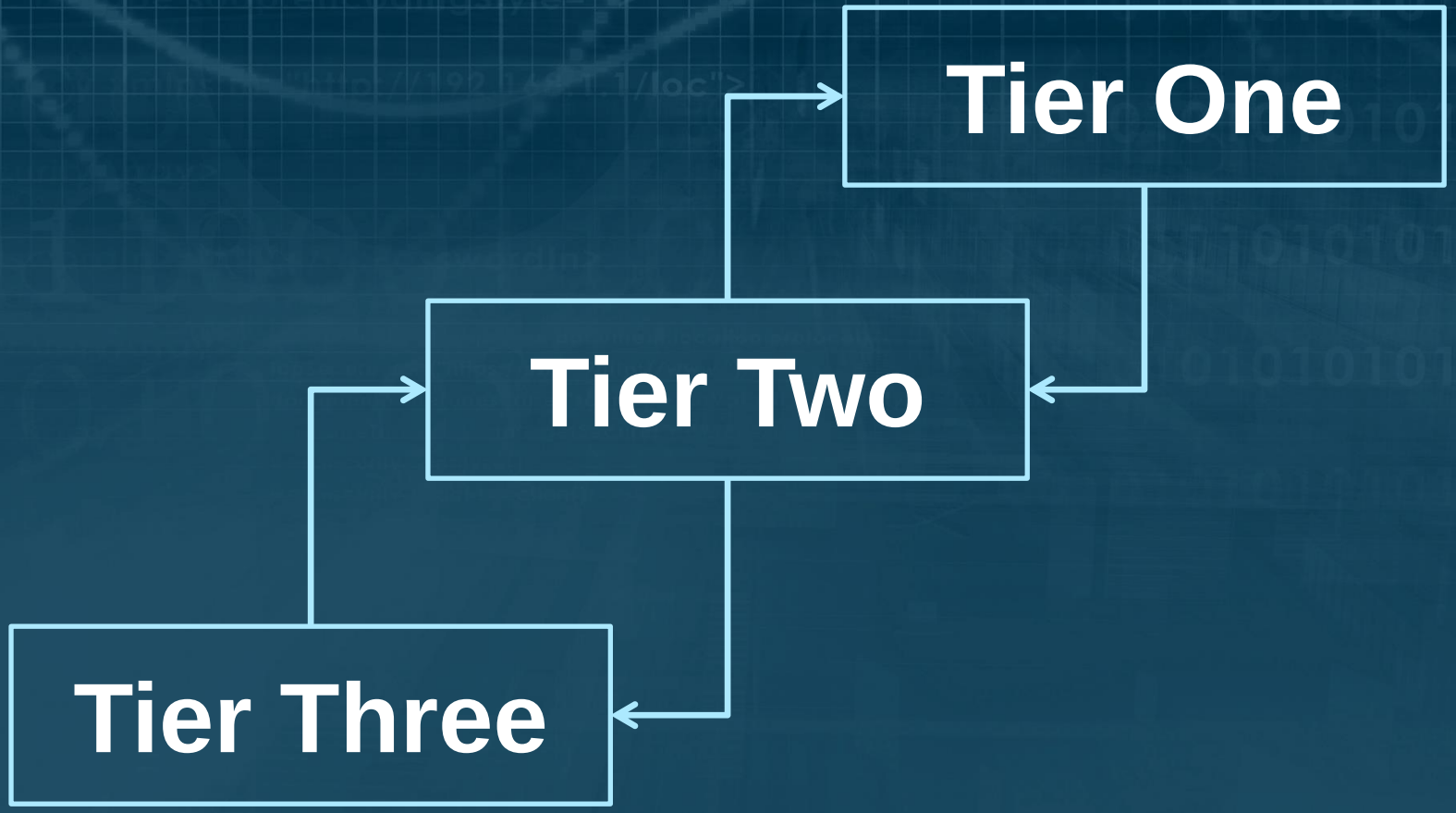
- **HTML file that conveys:**
  - Application name
  - Application version
  - Application patch level
- **ISO/IEC Standard – anyone can create SWID tags!**
  - Vendors can create and register SWIDs for their applications
  - Software tool can look at what is install on endpoint and create SWIDs
- **Stored in canonical location, so everyone knows where to look for SWIDs**

Compliant and Connected




UNCLASSIFIED
UNCLASSIFIED

DoD Network Hierarchy



Mitigations

Router

Web Server

CA

Mac Endpoint

VPN Gateway

Domain Controllers

Linux Endpoint

Windows Endpoint


virus alert!
malware
attack
25%
phishing
trojan
virus


FUTURE

For More Information

TCG TNC Endpoint Compliance Profile and FAQ

- http://bit.ly/15pH7K3
- IF-IMV 1.4- http://bit.ly/1fe1bRh
- PDP Server Discovery and Validation- http://bit.ly/18fsmr7
- SWID Messages and Attributes for IF-M- http://bit.ly/16L2KV9