Cybersecurity and You . . . Yeah You!

Joe Cupano
Consulting Product Manager, Dell EMC

Trust

- Senses
- Family
- Friends
- Other Contacts

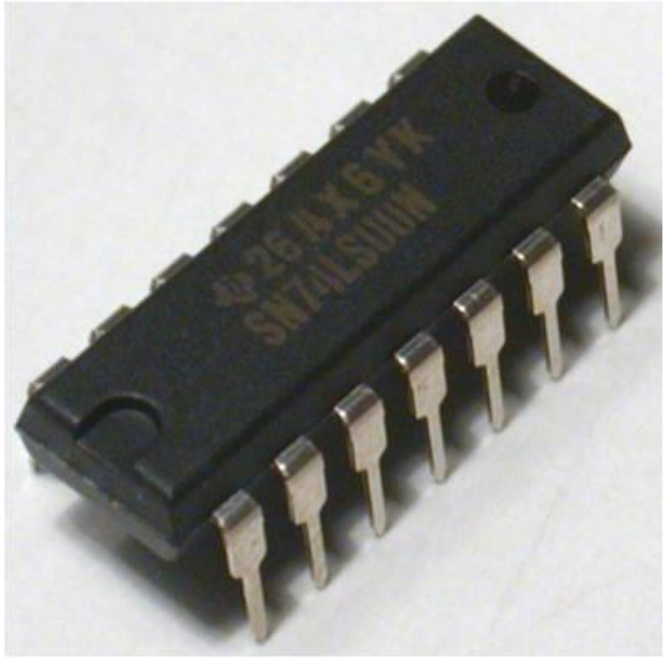
Reputation

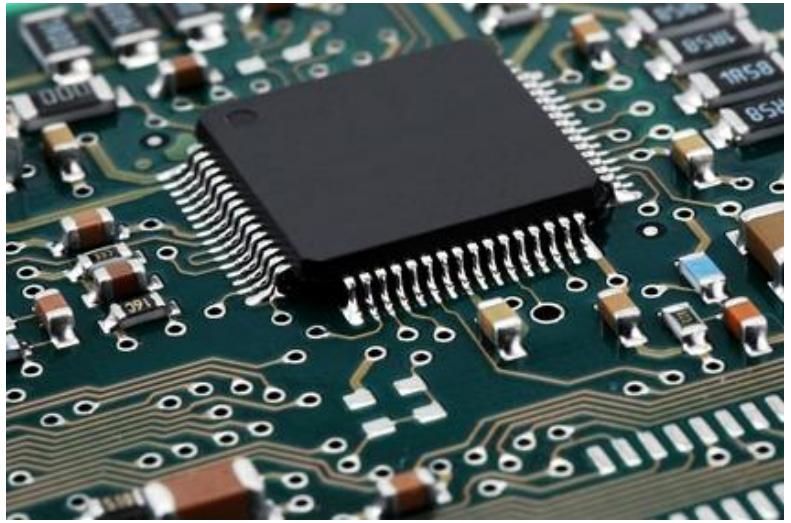
Trust in Hardware

- Circuits
- Tubes
- Transistors

Trust in Hardware

- Circuits
- Tubes
- Transistors
- Integrated Circuits
- Processors





Trust in Compute

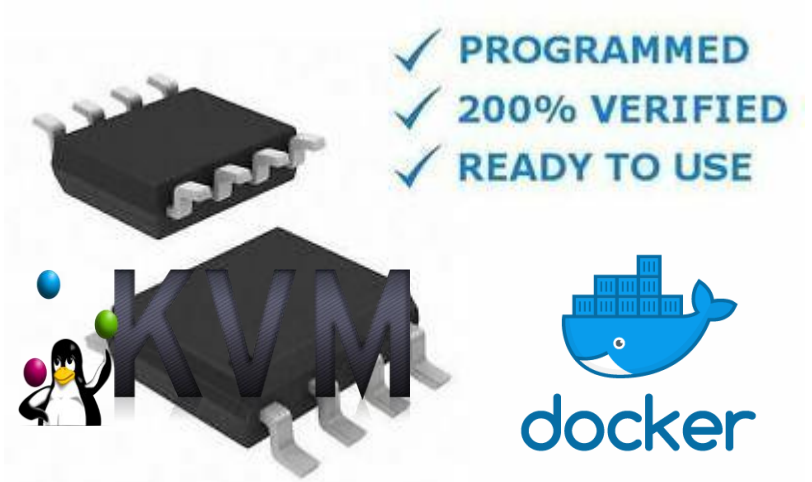
- Colossus
- Mainframes
- PCs and Laptops
- Servers

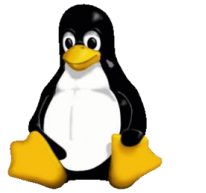
Trust in Compute

- Colossus
- Mainframes
- PCs and Laptops
- Servers
- Cloud Service Providers
- Mobile Devices

Trust in Software

- Firmware
- Operating Systems
  - Virtual Machines
  - Containers
- Languages
  - Compiled & Interpreted
- Frameworks and Platforms
  - Including SDK and IDE





Trust at risk of looking like this

Frameworks & Platforms -

Languages -

Operating Systems -

Compute (PC, Servers, CSP) -

Hardware (Firmware) -

Vulnerabilities

HVTECHI

Frameworks & Platforms

WordPress

CVE-2019-9864	PHP Scripts Mall Amazon Affiliate Store 2.1.6 allows Parameter Tampering of the payment amount. **Published:** March 28, 2019; 11:29:00 AM -04:00	*V3:* 6.5 MEDIUM *V2:* 4.0 MEDIUM
CVE-2019-1010257	An Information Disclosure / Data Modification issue exists in article2pdf_getfile.php in the article2pdf Wordpress plugin 0.24, 0.25, 0.26, 0.27. A URL can be constructed which allows overriding the PDF file's path leading to any PDF whose path is known and which is readable to the web server can be downloaded. The file will be deleted after download if the web server has permission to do so. For PHP versions before 5.3, any file can be read by null terminating the string left of the file extension. **Published:** March 27, 2019; 03:30:11 PM -04:00	*V3:* 9.1 CRITICAL *V2:* 7.5 HIGH
CVE-2019-1000031	A disk space or quota exhaustion issue exists in article2pdf_getfile.php in the article2pdf Wordpress plugin 0.24, 0.25, 0.26, 0.27. Visiting PDF generation link but not following the redirect will leave behind a PDF file on disk which will never be deleted by the plug-in. **Published:** March 27, 2019; 02:29:00 PM -04:00	*V3:* 7.5 HIGH *V2:* 5.0 MEDIUM

https://nvd.nist.gov/vuln/search

Frameworks & Platforms

CVE-2019-5739	Keep-alive HTTP and HTTPS connections can remain open and inactive for up to 2 minutes in Node.js 6.16.0 and earlier. Node.js 8.0.0 introduced a dedicated server.keepAliveTimeout which defaults to 5 seconds. The behavior in Node.js 6.16.0 and earlier is a potential Denial of Service (DoS) attack vector. Node.js 6.17.0 introduces server.keepAliveTimeout and the 5-second default. **Published:** March 28, 2019; 01:29:01 PM -04:00	(not available)
CVE-2019-10061	utils/find-opencv.js in node-opencv (aka OpenCV bindings for Node.js) prior to 6.1.0 is vulnerable to Command Injection. It does not validate user input allowing attackers to execute arbitrary commands. **Published:** March 25, 2019; 09:29:00 PM -04:00	(not available)
CVE-2018-11798	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path. **Published:** January 07, 2019; 12:29:00 PM -05:00	*V3:* **6.5 MEDIUM** *V2:* **4.0 MEDIUM**
CVE-2018-12123	Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Hostname spoofing in URL parser for javascript protocol: If a Node.js application is using url.parse() to determine the URL hostname, that hostname can be spoofed by using a mixed case "javascript:" (e.g. "javAscript:") protocol (other protocols are not affected). If security decisions are made about the URL based on the hostname, they may be incorrect. **Published:** November 28, 2018; 12:29:00 PM -05:00	*V3:* **4.3 MEDIUM** *V2:* **4.3 MEDIUM**

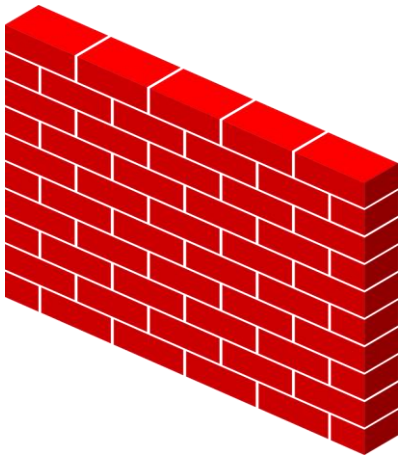
Languages

CVE-2019-9948	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call. **Published:** March 23, 2019; 02:29:02 PM -04:00	*V3:* 9.1 CRITICAL *V2:* 6.4 MEDIUM
CVE-2019-9947	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string or PATH_INFO) followed by an HTTP header or a Redis command. This is similar to CVE-2019-9740. **Published:** March 23, 2019; 02:29:02 PM -04:00	*V3:* 6.1 MEDIUM *V2:* 4.3 MEDIUM
CVE-2019-7537	An issue was discovered in Donfig 0.3.0. There is a vulnerability in the collect_yaml method in config_obj.py. It can execute arbitrary Python commands, resulting in command execution. **Published:** March 21, 2019; 04:29:01 PM -04:00	*V3:* 9.8 CRITICAL *V2:* 7.5 HIGH

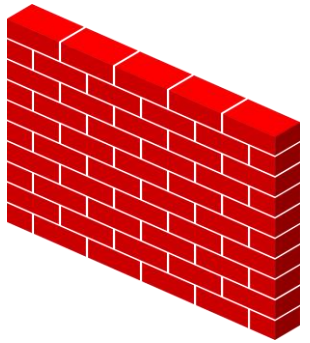
Operating Systems

- Linux, FreeBSD, Windows, etc
- Virtualization
  - Intel , AMD, ARM
- Containers
  - Docker, Mesos, LXC, etc

Reducing Risk

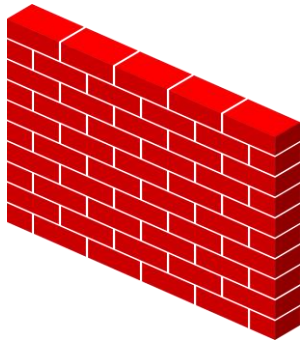


Fundamental Concepts



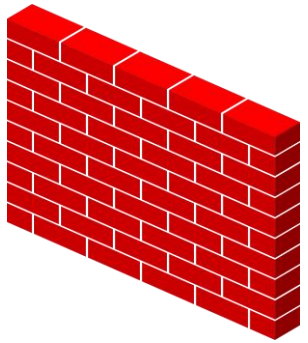
- Confidentiality
  - Encryption at-rest and in-flight
- Integrity
  - Non-repudiation
- Availability
  - Keeping the lights on and systems/data accessible

Fundamental Practices



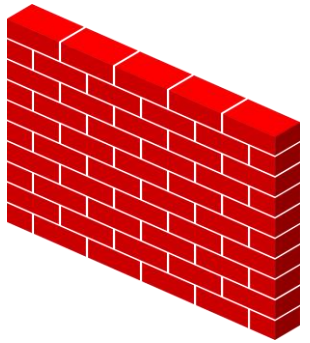
- Identity
- Authentication
- Authorization
- Audit

Know your Assets



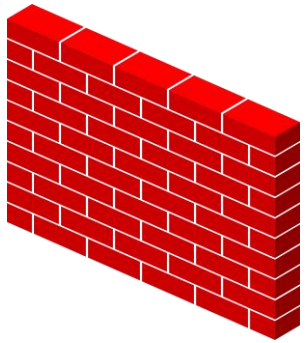
- Classification
  - Public, Restricted, Customer Confidential, Internal Only
- Ownership
  - Data, System, RACI
- Retention
- Controls
  - Chain of Custody

Know your Environment



- Architecture
  - Systems, Network, Tenancy (Cloud)
- Threat Profile
  - Given the chains of assets required for a customer application, what are the potential threats to each “link” and to the chains as a whole
- Dependencies
  - Data Sources, Cloud Availability, etc.

Know your Obligations



- Service Levels
- Legal
- Compliance
- Privacy

Cybersecurity

- **Fundamentals**
  - Authentication, Authorization, Audit
  - Confidentiality, Integrity, Availability
  - People, Policy, Process, Data, Technology
- **Risk**
  - Drivers – Business or Regulatory
  - Analysis – Threat, Vulnerability, Asset Value
  - Manage – Reduce, transfer, Accept
- **Policies & Procedures**
  - Statements, Policies, Standards, Baselines, Guideline, operations procedures
- **Training, Education, & Awareness**
- **Implementation**
  - Assess Risk
  - Positive identity
  - Authorized access (“need to know”)
  - Secure products
  - Layered defense
  - Data-centric
- **Assure (“Trust but verify”)**

- **Security**
  Architecture, Virtual Private Network (VPN), Network Intrusion Management, Wireless Security, Firewalls, IPS, IDS
- **Identity management and access control**
  User ID and Password Management, Authentication, Web Access Control, PKI
- **Platform Security**
  Vulnerability Management, OS security, Secure Data Storage
- **Application Security**
  Email Security, Web Security, Secure Instant Messaging, Application Firewalls, Database Security, Secure Software Development
- **Open Source Security Tools**
- **Security Threats**
  Viruses, worms, malware, Email, Web, Emerging Information Security Threats, Identity Theft
- **Security Management**
  Regulatory Compliance, Information Security Standards, Laws, Investigations and Ethics
- **Information Security Careers, Training and Certifications**

http://www.mindcert.com/category/mind-maps/cissp/

Questions?

joe@cupano.com

OpenHub
Innovation | Collaboration | Education

SUNY ORANGE

Mount Saint Mary College

ORANGE COUNTY NEW YORK
1 NOVEMBER 1683

Building an Open Source Cyber Range in the AWS

by Thomas Capetta (bio below)

The CyberRange project was created to provide technologists interested in Cyber Security, Cloud Computing, and DevOps a safe training environment. The goal of building an automated and bootstrapped training environment, full of vulnerable machines, in less than 10 minutes. The CyberRange provides a bootstrap framework for a complete offensive, defensive, reverse engineering, and security intelligence tooling in a private research lab using the AWS Cloud

Presentation will include an overview of the common challenges of Cyber Security Researchers, outline the barriers of entry for training across disciplines and how to leverage open-source tooling to overcome them.

https://www.tfaforms.com/4768012

HVTECHFEST 2019

OpenHub
Innovation | Collaboration | Education

SUNY ORANGE

Mount Saint Mary College

ORANGE COUNTY
NEW YORK
1 NOVEMBER 1683

Certifications

(ISC)²®

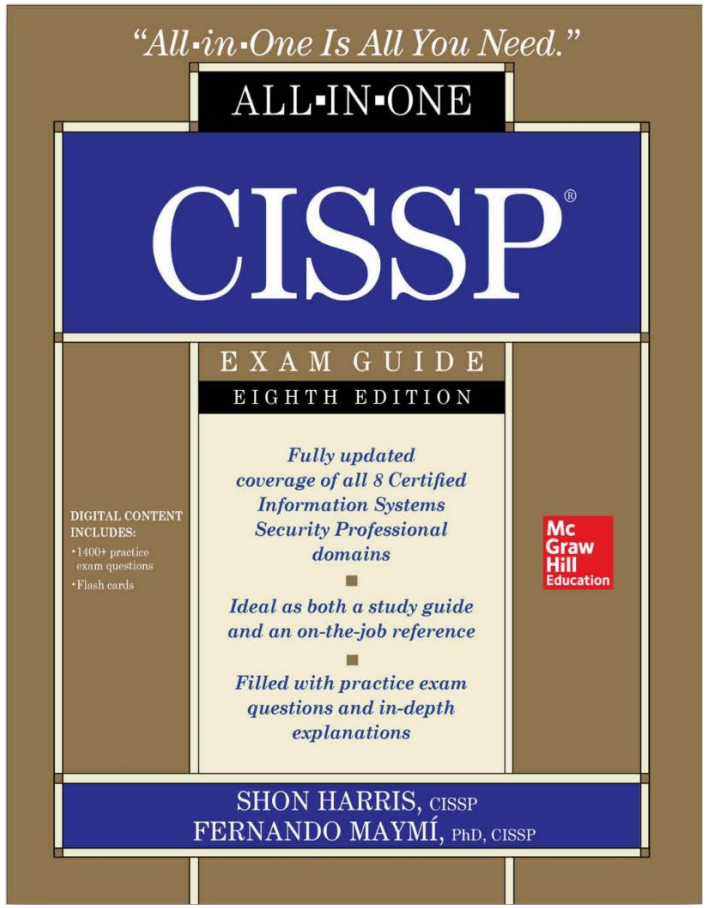
(ISC)² CERTIFICATIONS

- CISSP — LEADERSHIP & OPERATIONS
- SSCP — SECURITY ADMINISTRATION
- CCSP — CLOUD SECURITY
- CAP — AUTHORIZATION
- CSSLP — SOFTWARE SECURITY

(ISC)²: The World's Leading Cybersecurity and IT Security Professional Organization

You face immense pressure to stay ahead of attacks and up-to-date in our ever-changing security profession. But you aren't alone.

(ISC)² is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 140,000 certified members strong, we empower professionals who touch every aspect of information security.

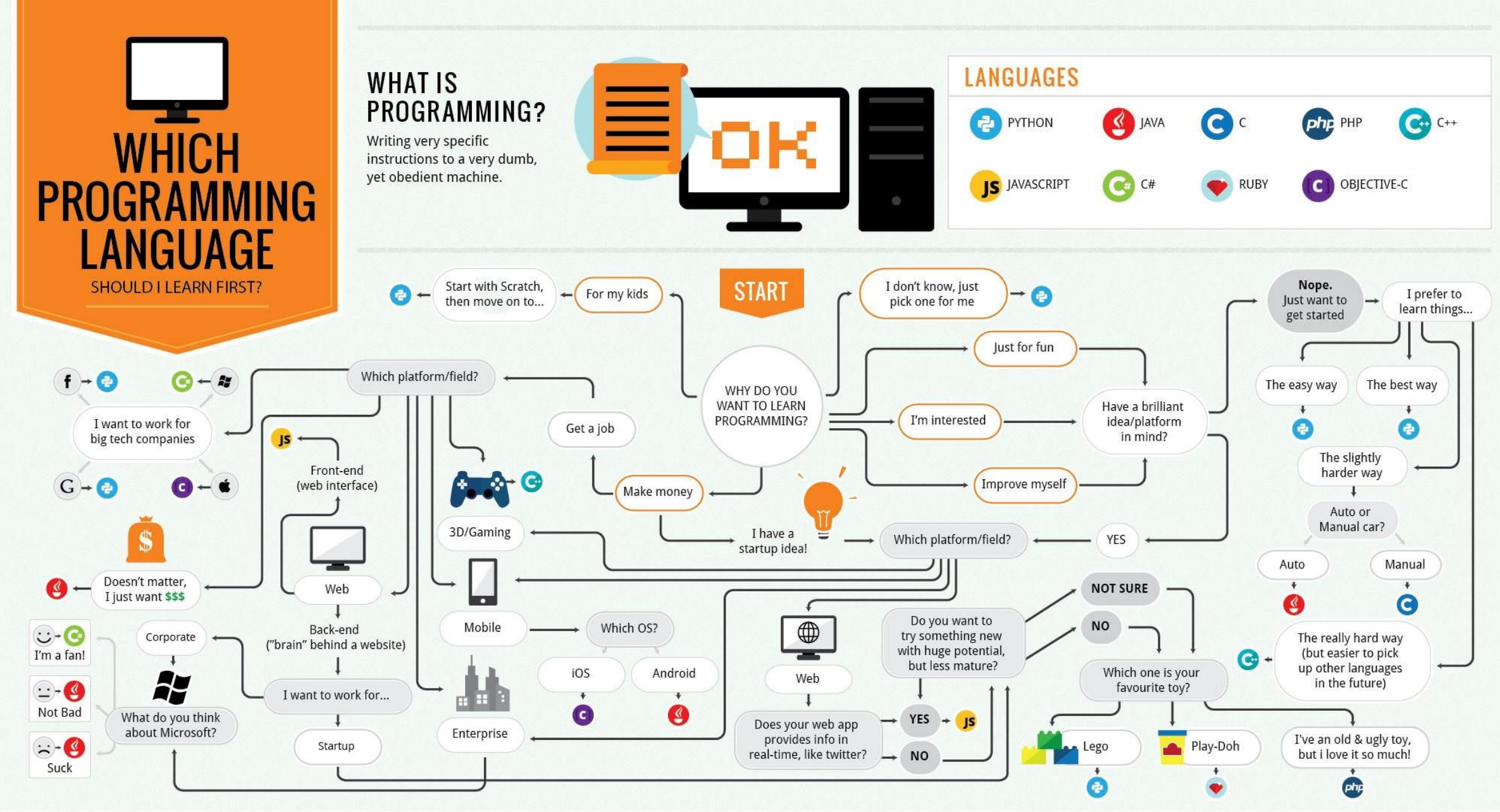


https://www.isc2.org

CompTIA

CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

https://certification.comptia.org/certifications/security



https://hackernoon.com/top-3-programming-language-to-watch-out-in-2019-95995e81ad2b