Office of the Washington State Auditor
Pat McCarthy

My Journey through IT and Cybersecurity

A humble career path

Shaun Marquardt, MCL, CISSP
Cybersecurity Architect

Shaun.Marquardt@sao.wa.gov

October 30, 2023

CISSP®

MASTER OF CYBERSECURITY & LEADERSHIP
UNIVERSITY of WASHINGTON | TACOMA

About Your Speaker

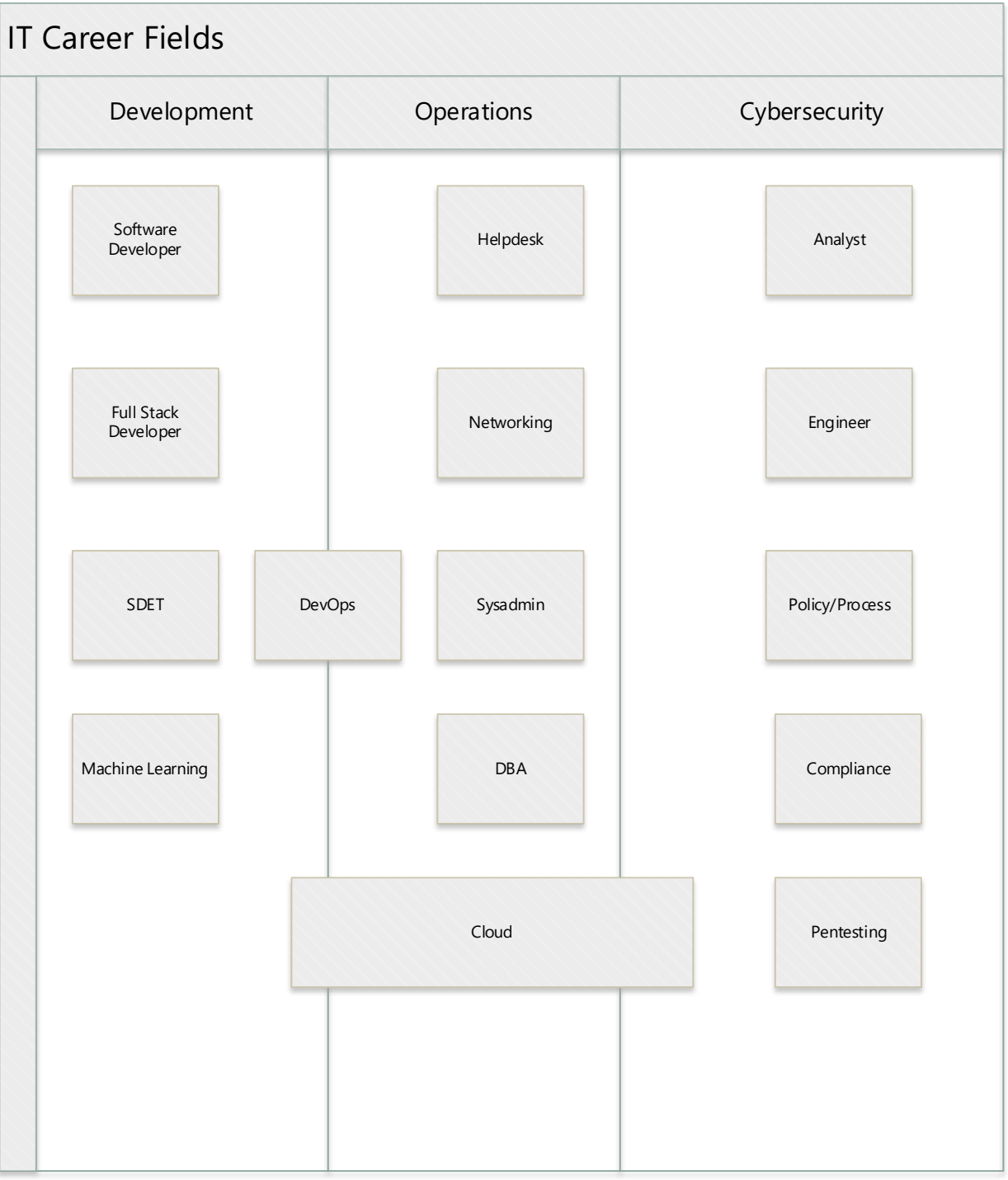
- 18+ Years of IT Experience
- Master of Cybersecurity and Leadership (MCL), University of Washington
- CISSP https://www.isc2.org/Certifications/CISSP
- https://www.credly.com/badges/0b8ac5fc-3457-4708-a8b0-0d10e89d14c5/public_url

In The Beginning

- 1990/2000
- 2001-2002 Technical College, Associate's Degree
  - ✓ A+ | Network+ | Linux+ | CCNA | Novell NetWare 5.1 | MCP Windows 2000 Server
- And then … I had a hard time getting a job in the IT space. So:
- 2005-2012: United States Army – Start of IT Experience. 8 years
  - ✓ Domain Admin All Army Okinawa & IT Security
  - ✓ Network Operations Manager
  - ✓ Hospital Information Systems Admin | Sec+
  - ✓ Senior Infosec Manager

After the Army…

- 2012-2013: Small private consulting company out of Seattle | VCP, MCP
- 2014: Contractor for Microsoft
- 2015: State of Washington
  - ✓ eDiscovery/Forensics
  - ✓ Enterprise AD | ITIL Foundations, CSM
  - ✓ Senior Infosec Engineer | CISSP
  - ✓ Principal Cybersecurity Architect | MS-Azure
- Used GI Bill:
  - ✓ 2021: Graduated UW Tacoma Bachelors of Science Information Technology
  - ✓ 2022: Graduated UWT Masters of Cybersecurity and Leadership, double honors



So, what's my path?

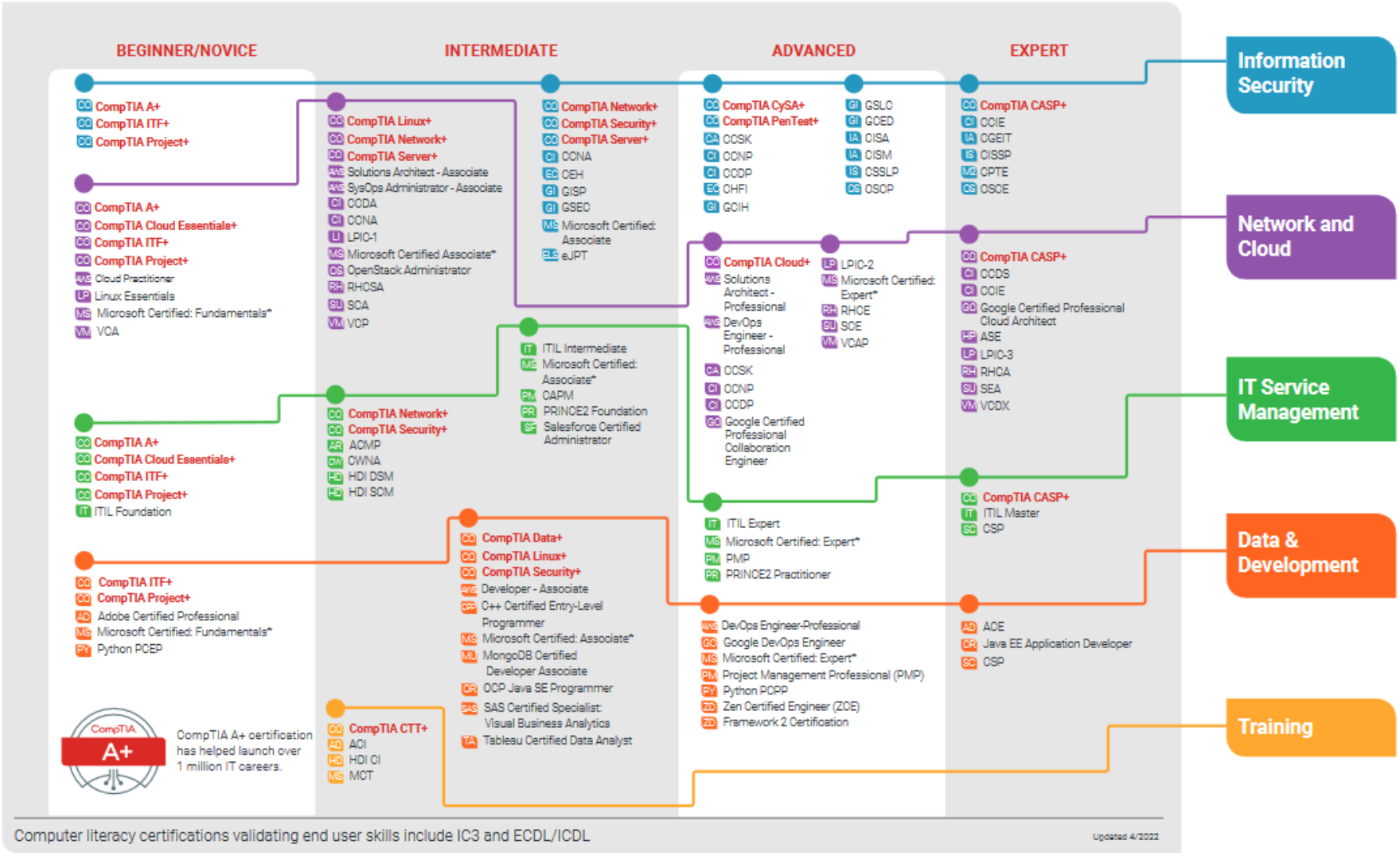
CompTIA IT Career Roadmap

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at:
CompTIA.org/CertsRoadmap

CompTIA

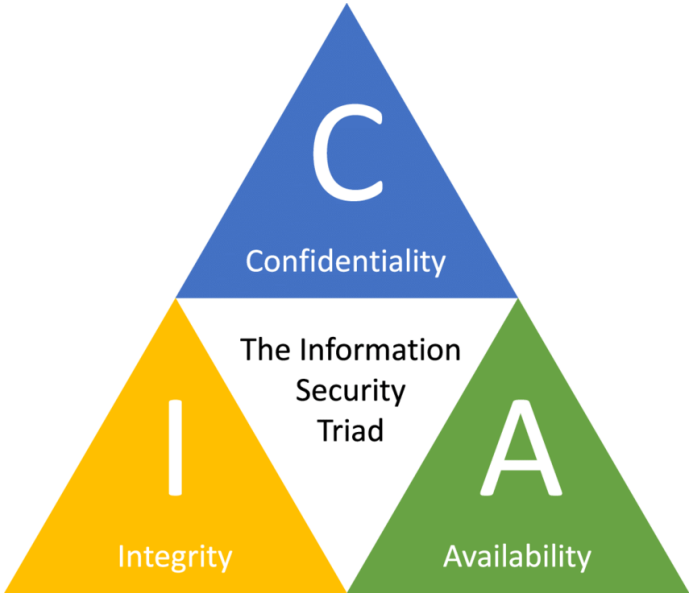
Certifications validate expertise in your chosen career.



Microsoft provides three certification paths. Please visit Microsoft's webpage for a full list of their offerings: https://bit.ly/3tJYm8Z

Intro to Cybersecurity
- What is Cybersecurity?

- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

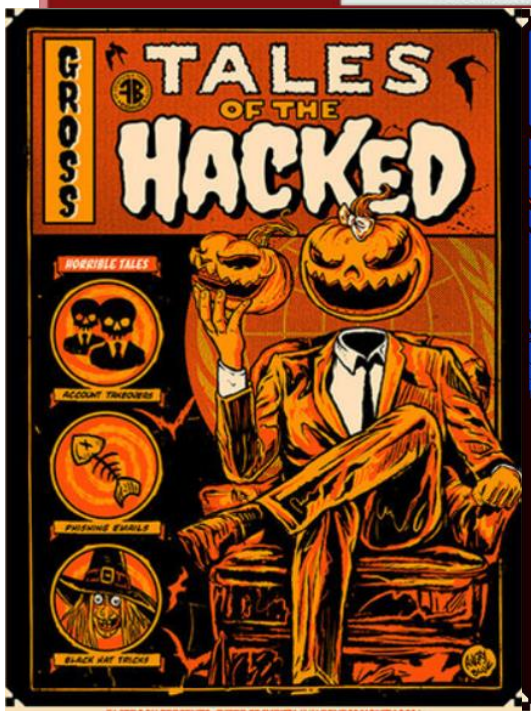


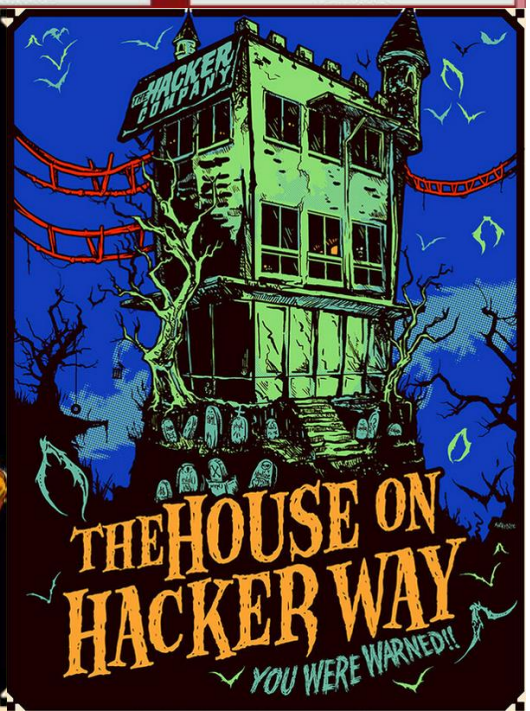
A Few Definitions

- Threat: *any* potential danger that is associated with the exploitation of a vulnerability.
- A vulnerability is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications, unenforced password management…

Threats

- Virus
- Worm
- RAT
- Ransomware
- Social Engineering
- Data Exfiltration
- Phishing

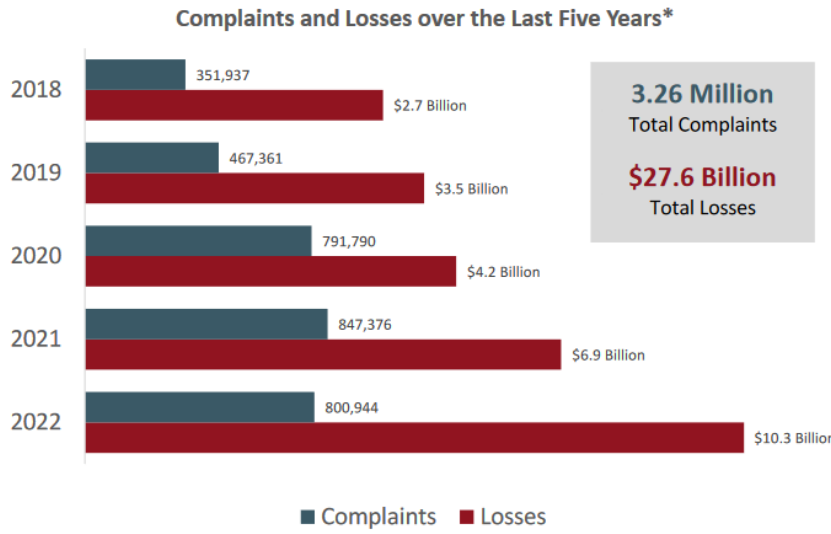


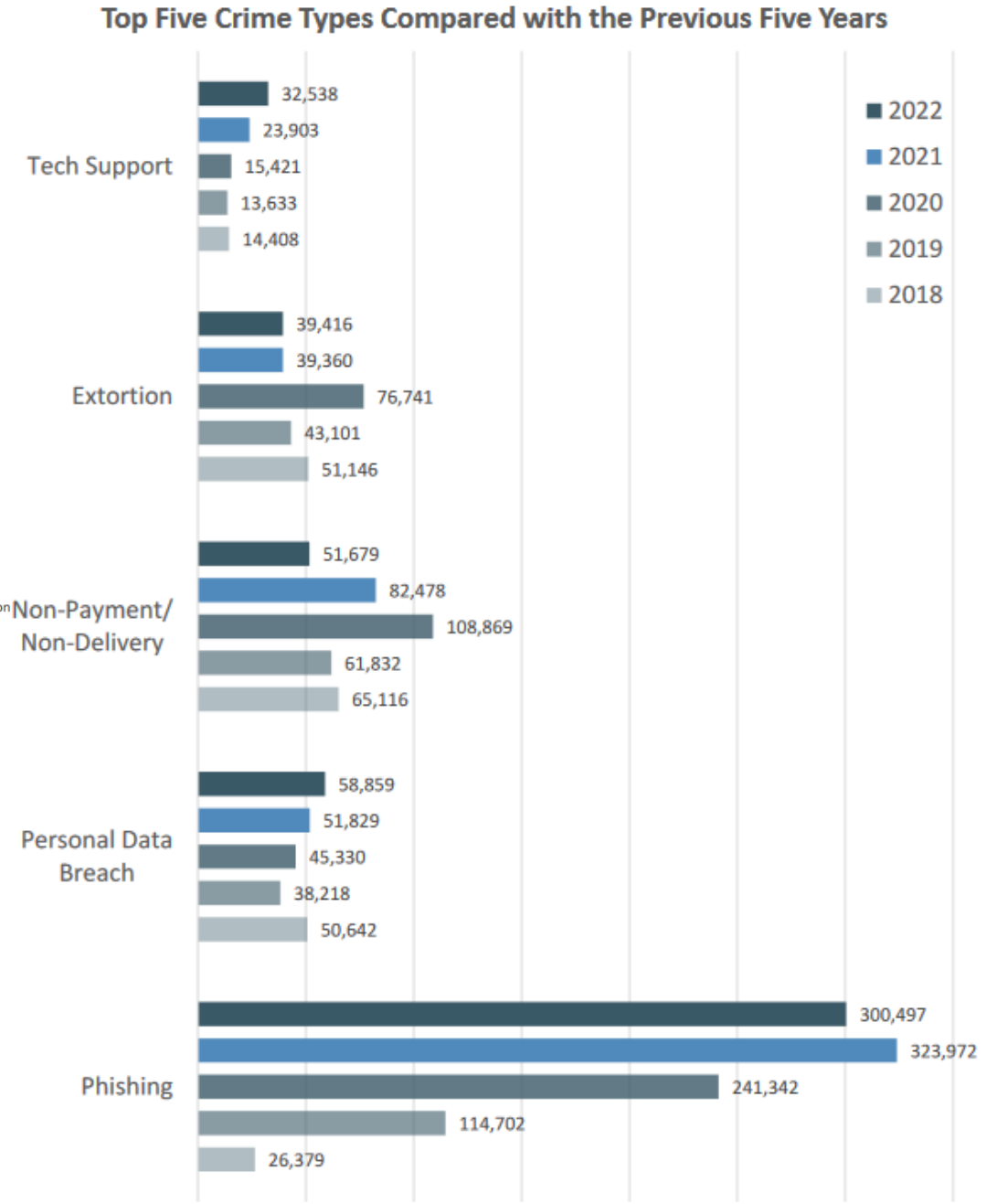


Why Cybersecurity?

- Cybersecurity is inexorably tied to software development and application security. It is a risk management and reduction function to the business.
- Pays very well (80-90k start), no job shortage
- Common application misconfigurations:
  - ✓ Buffer overflow
  - ✓ Misconfigurations
  - ✓ Plain text credentials
  - ✓ Injections

Let's Talk About Risk





Source: 2022 FBI Internet Crime Report: 300,497 victims of phishing. 2021 323,972 victims

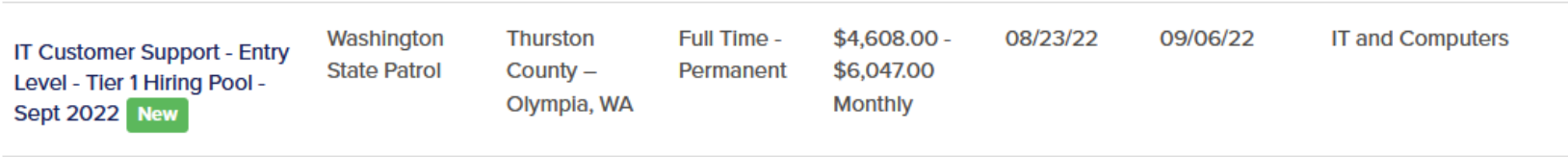
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Project Showcase

- RDA Hippa Risk Analysis
  - ✓ Conducted over 9 systems to satisfy the statutory requirement regarding the storage, processing, and reporting of confidential client data.
  - ✓ Perform composite risk analysis according to the risk analysis questionnaire
  - ✓ Access, recommend, and log corrective action plans for future implementation
- SIEM Projects
- Security Design Reviews
  - ✓ ZenDesk, MS Data Gateway, Arctic Wolf
- Secure Desktop Configuration

Shameless Plug

- https://careers.wa.gov/
  - ✓ Filter: “IT and Computers”
  - ✓ Sort: Salary Lowest to Highest
  - ✓ https://www.governmentjobs.com/careers/washington?category[0]=IT%20and%20Computers&sort=Salary%7CAscending



IT Customer Support - Entry Level - Tier 1 Hiring Pool - Sept 2022 New	Washington State Patrol	Thurston County – Olympia, WA	Full Time - Permanent	$4,608.00 - $6,047.00 Monthly	08/23/22	09/06/22	IT and Computers

Also look for positions listed as “In Training”

An internship might also be a great opportunity for you.

Jokes

What do hackers do when they go on vacation?

They go phishing!

HA, HA, HA
HA, HA, HA
HA, HA, HA

- Why do hackers grow their plants with hydroponics?
- To get root access.

HA, HA, HA
HA, HA, HA
HA, HA, HA

Two Wi-Fi engineers got married.

The reception was fantastic

HA, HA, HA
HA, HA, HA
HA, HA, HA

- Why couldn't the hacker cross the sea?
- The port was closed.

HA, HA, HA
HA, HA, HA
HA, HA, HA

Contact Information

Contact Shaun Marquardt,

shaun.marquardt@sao.wa.gov

(564) 201-2978

https://www.linkedin.com/in/smarquardt

Website: www.sao.wa.gov

Twitter: *@WAStateAuditor*

Facebook: www.facebook.com/WAStateAuditorsOffice

LinkedIn: *Washington State Auditor's Office*

Before I get into open questions…

- "How to bypass an Antivirus?"
  - ✓ What is an Antivirus & How it works
    - Primarily Signature based
    - Heuristic scanning looks for commands that may indicate malicious intent without a signature.
- For Educational Purposes Only
  - ✓ Write a Zero Day.
  - ✓ Powersploit framework: AV Bypass Module

Questions