Gaucho Security Operation Center

Martin Bencic
Glendale Community College AZ
martin.bencic@gccaz.edu
623.845.3237

6/8/23

Glendale's Cybersecurity program

Curriculum

- ✓ Center of Academic Excellence in Cyber Defense NSA.
- ✓ US Cyber Command Academic Network member: Academic Engagement Network
- ✓ Gaucho Cyber Cave: Proprietary Warfare Range
- ✓ EC-Council Academic Partner
- ✓ Red Hat Academy
- ✓ CompTIA Academy
- ✓ Palo alto Networks
- ✓ VMWare Academy

Offensive/Defensive security

- ➢ Utilize training and competitions from National Cyber League and Cyber Skyline curriculum.
- ➢ Participate in Regional and National Collegiate Cyber Defense Competitions. As real-world as it gets.
- ➢ Gaucho Cyber Cave: Real world scenarios with intentionally created environments with built-in vulnerabilities.

AAS 3197 Cybersecurity degree

Core all Required

- Survey of CIS
- Windows Admin
- Linux Sys Admin I
- IT Ethics
- Python
- Networking
- **Information Security**
- **Ethical Hacking**

Track 1

Cyber Ops

- A+ Prep
- **Linux Sys Admin II**
- IT Forensics
- **IT Adv Forensics**
- Internship

Track 2

Linux Adm

- Linux Admin II
- Linux Scripting
- Linux Net Admin
- Linux Security
- Linux Capstone

Track 3

Cloud Sys Admin

- PowerShell
- Azure Admin
- Azure Dev Ops

Track 4

Networking

- Switch/Routing
- Enterprise
- Firewall
- Security

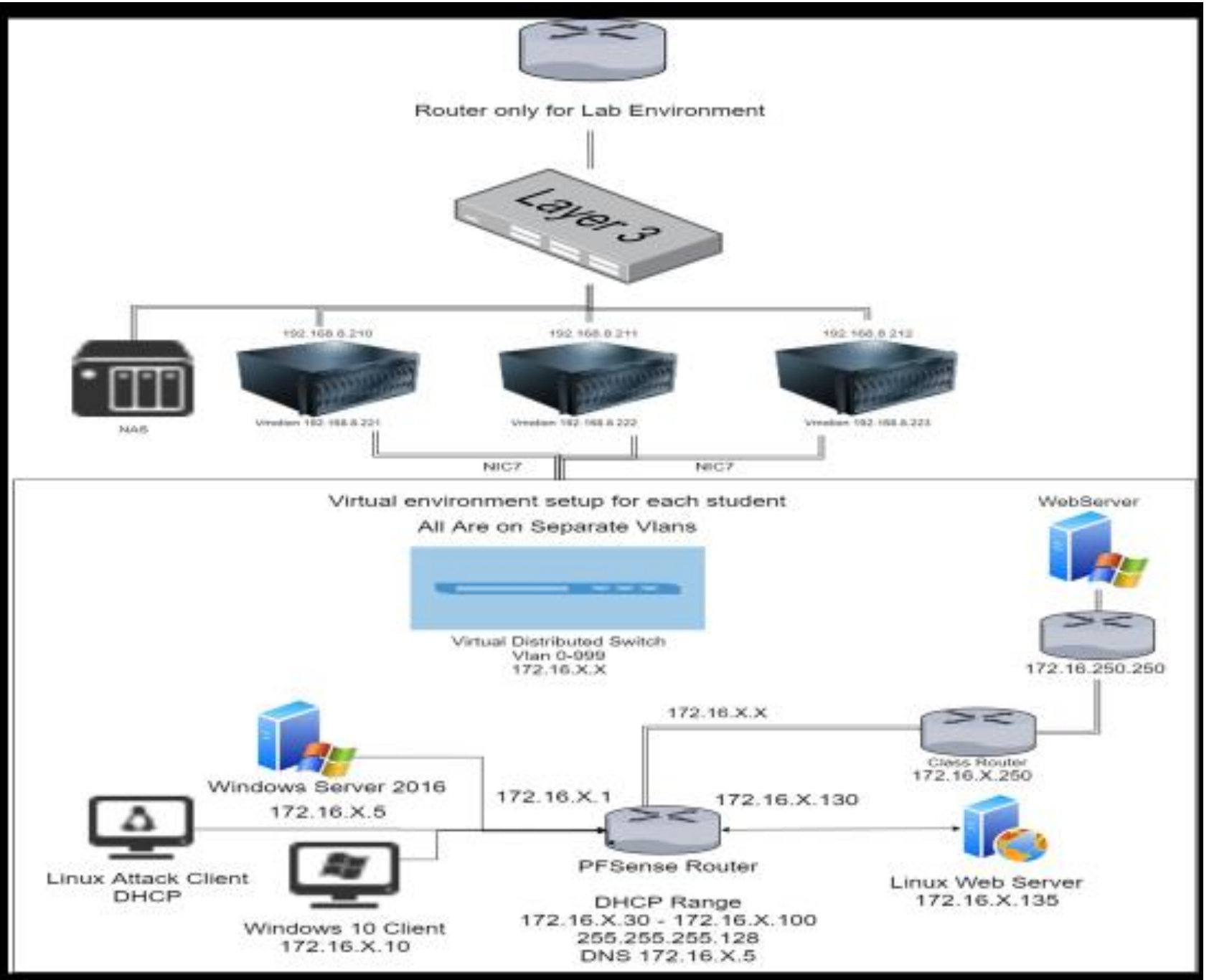
Track 5

Engineering

- SQL
- C Programming
- Programming II
- Assembler
- Linux Admin II
- MIS

(Bold) Certification Eligible: CCNA, Security +, RHCSA, CEH, CHFI, CySA+

Gaucho Cyber Cave



Which is more accurate?

1. Knowledge + Simulation Skill Development = Career
2. Knowledge + Real World Skills = Competency which leads to Career

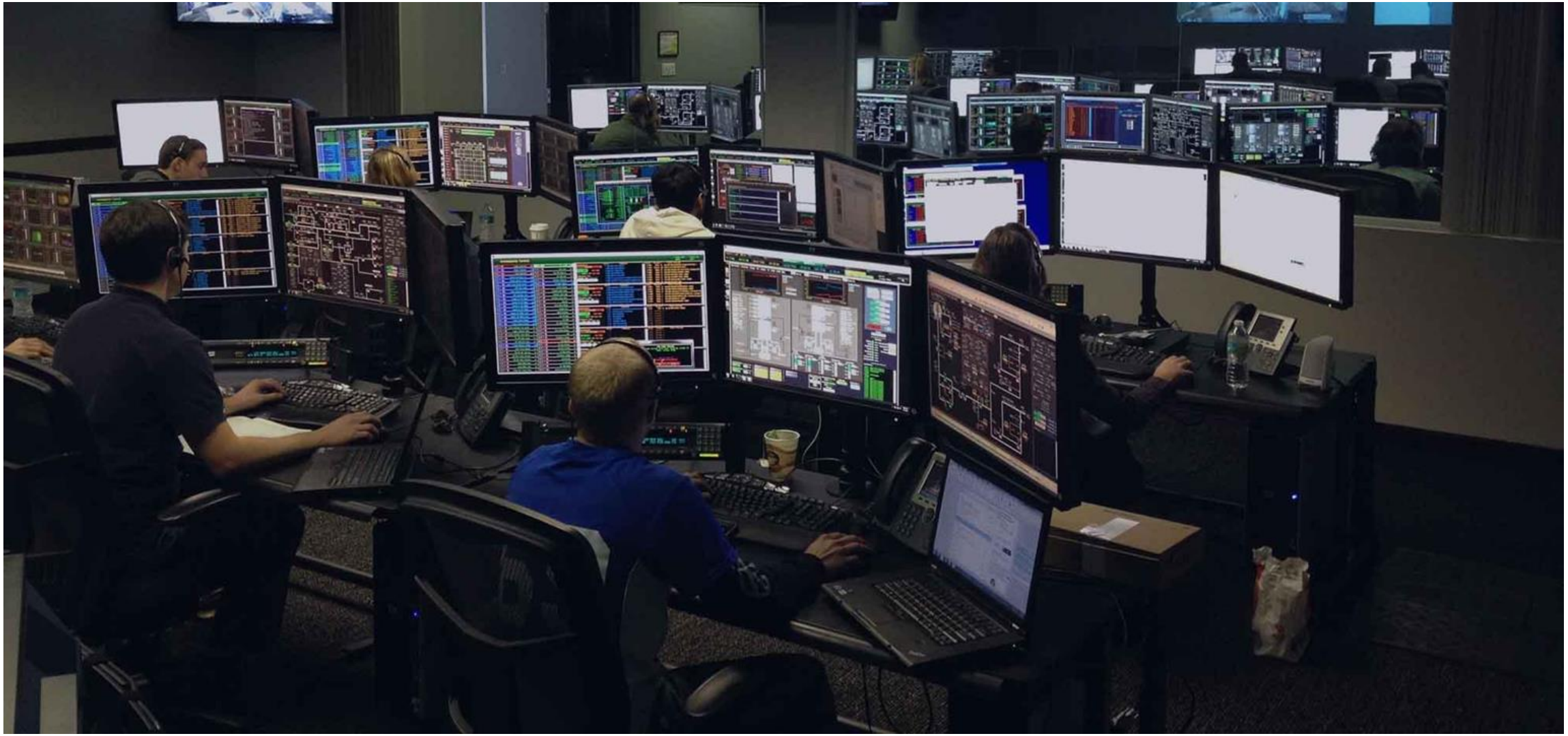
As we know the Simulation of Skills is not the same as Real World Skills. It is for this reason that we are building the GSOC.

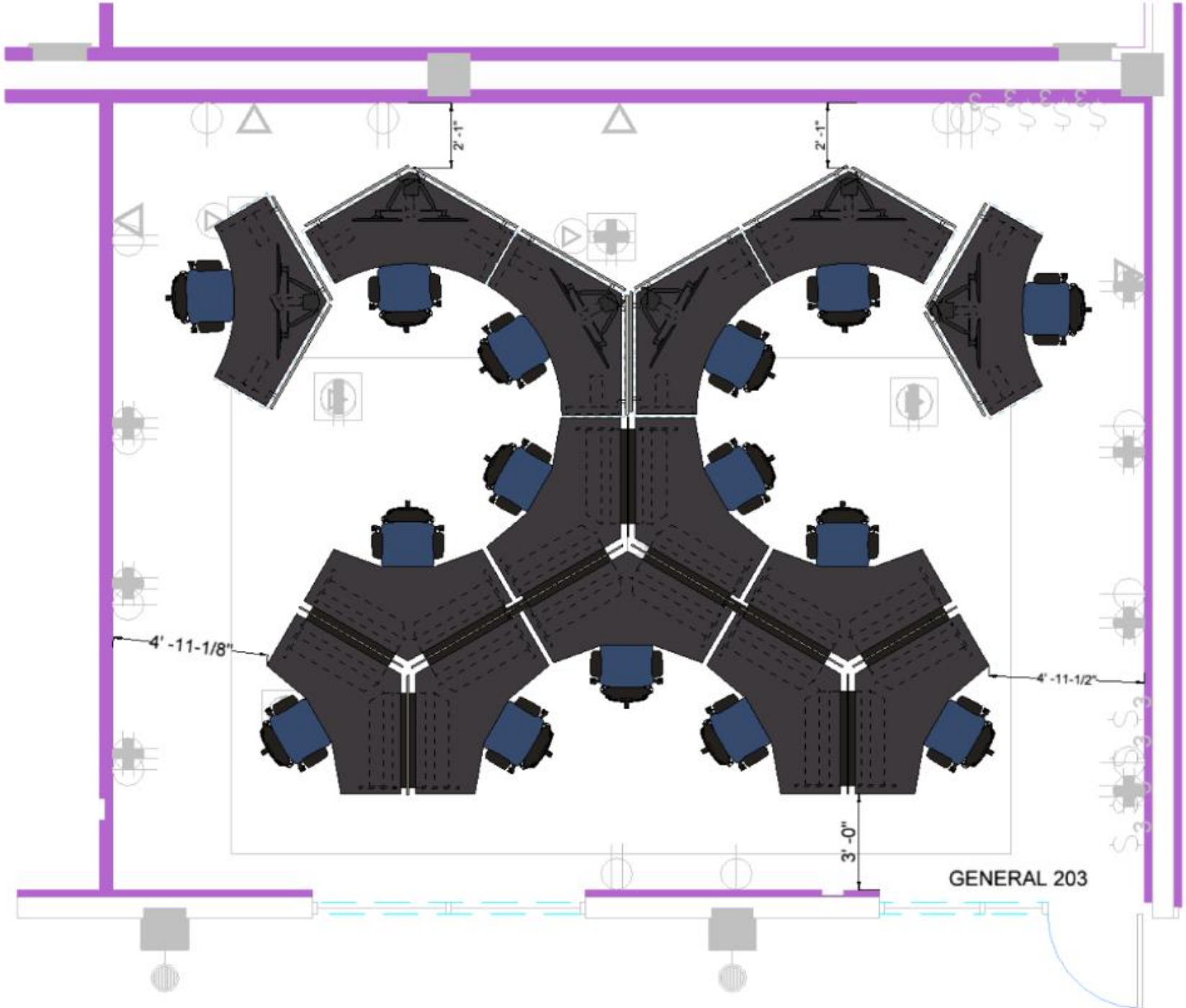
What’s in store:

Classroom like Configuration?

No!

Actual working environment?





Something in between GSOC Floor

Why create a SOC/Internship

1. Narrow the gap between academia and employment
2. Students inability to get placed in relevant field
3. Inability to get quality experience to enhance competency
4. We have no control over what they are learning off site
5. Management of student placement and associated documentation
6. Volume of placements needed is constantly growing

In short, we have to build our own environment in which we can control the above items.

Training Functionality

- Full service of industry vulnerabilities, security monitoring, alert ticket handling, incident triage, incident escalation, etc.
- Current industry: IPS/IDS, NTP, Data Collection, SIEM, etc.
- Traffic Generator
- Attacks with varying degree of difficulty/intensity
- NIST and NICE Workforce Framework
- Self paced training to earn opportunity for paid internship
- CySA+ certification opportunity

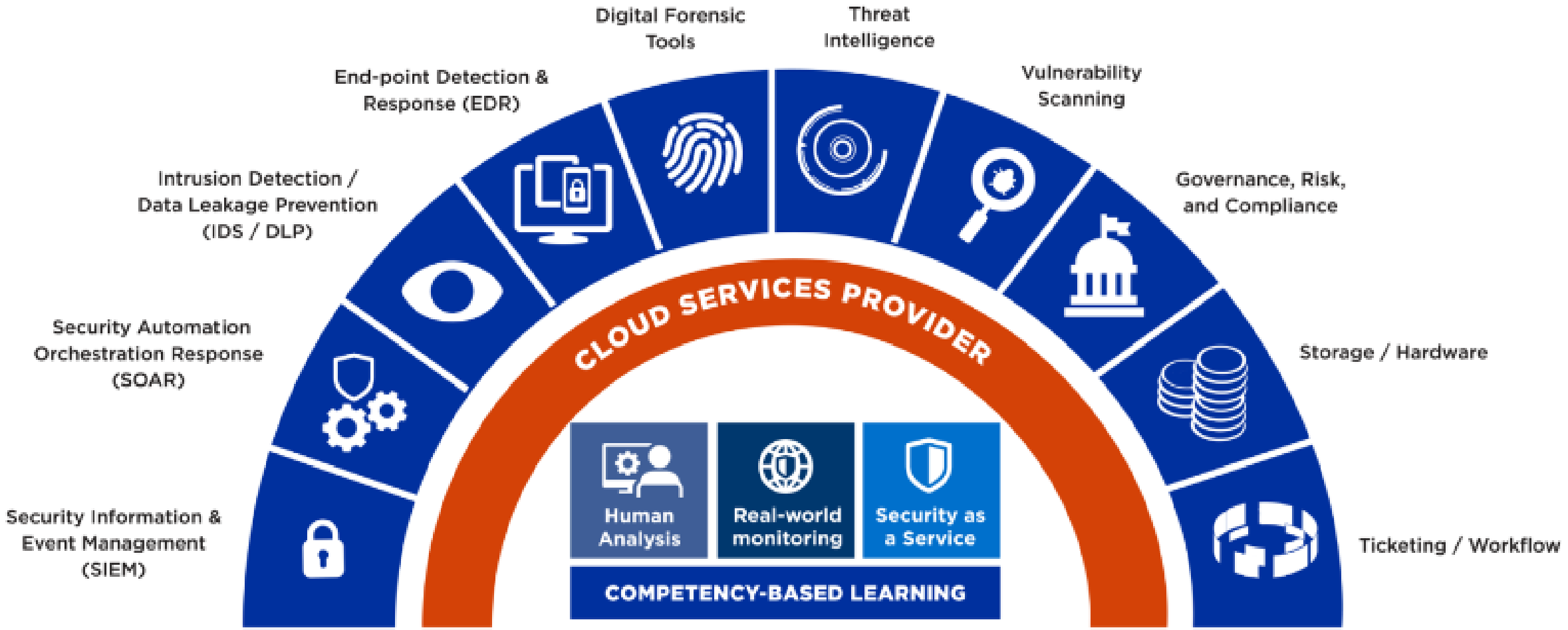
Paid Internship GSOC Environment

- Monitor-Detect-Inform
- Detailed MOU for services provided (next slide)
- Video Wall: ticketing, traffic, real time tracking
- Lead Analyst and Lead Engineer (Tier 2 analysts) Full time employees
- 12 student interns per semester (Tier 1 analysts)
  - Paid internship 300 hours per semester
  - 4 hour shift on floor
  - $345k paid student internship

Services Parameters

1. Not competing with industry. Learning environment not MSSP.
2. Clients must be below Cyber Poverty Level
3. Monitor: real time network traffic and resource analysis (Stellar Cyber)
   - Security Information and Event Manager (SIEM)
   - Network Detection & Response (NDR)
   - End Point Detection (EDR)
4. Service hours:
   - During semester
   - 5 days a week
   - 4 hours per day

Expanded Functionality



Micro-credentialing, competitions, badging

1. Micro-credentialing: industry recognized preparation Tier 1 SOC Analyst
2. Competition environments: i.e., Red Team vs Blue Team
3. Hosting (high school) outreach competitions
4. Corporate training sessions
5. Badging to include training for adjunct faculty/faculty
6. These can serve as alternate revenue stream(s)

Questions

Martin Bencic, MAEd
Glendale Community College
https://www.gccaz.edu/academics/departments/business/cybersecurity
martin.bencic@gccaz.edu
623.845.3237