



SRA @ RIT

Introduction to Cybersecurity

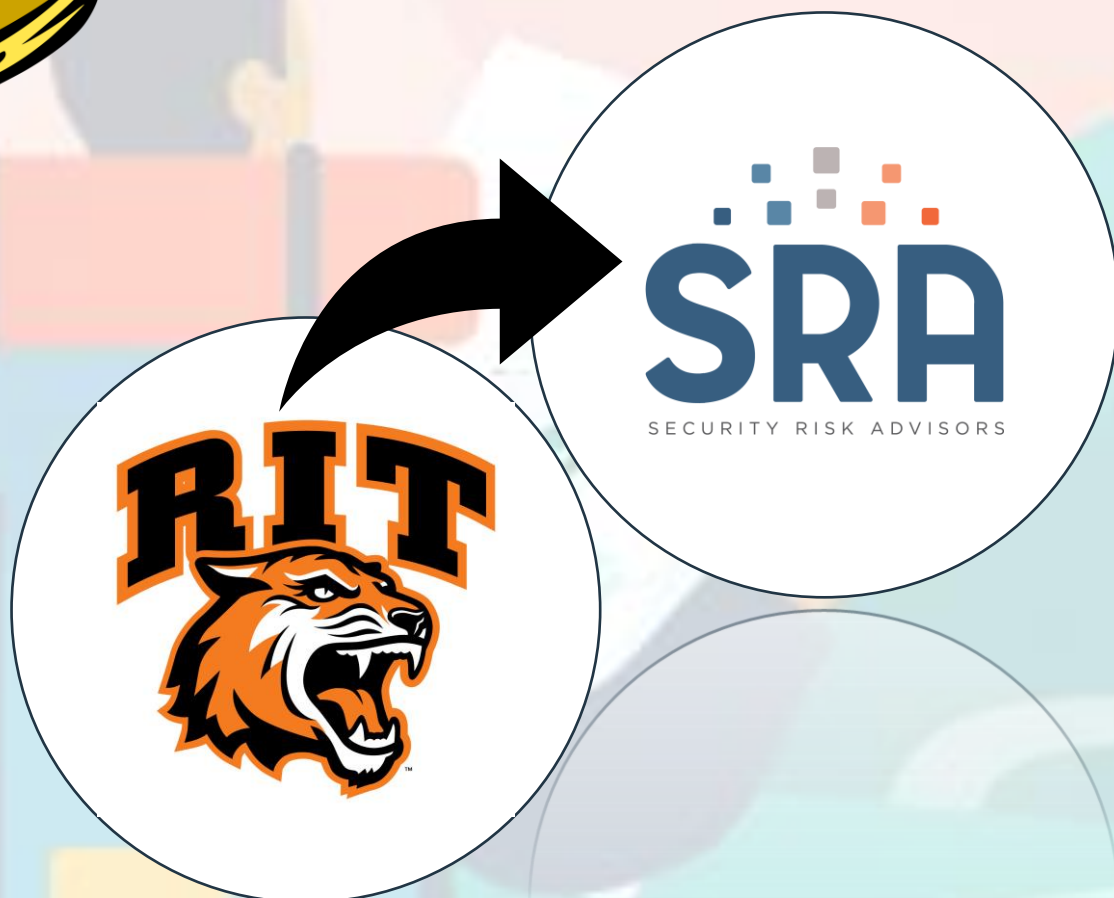
Joe Cicero

Director of Strategic Alliances





Mapping A Career in Cybersecurity



■ Why?



■ How do you get in?



■ Is it your passion?



■ So what?



"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers—organizing your lives, staying in touch with people, being creative—if we don't solve these security problems, then people will hold back."

— Bill Gates, 2002, Microsoft

...People were not held back, and the problems have grown exponentially...



State of Cybersecurity

- Threats are evolving
- Number of threat actors are growing
- Security products and services are not perfect
- Cybersecurity is a never-ending race



How can you join the mission?

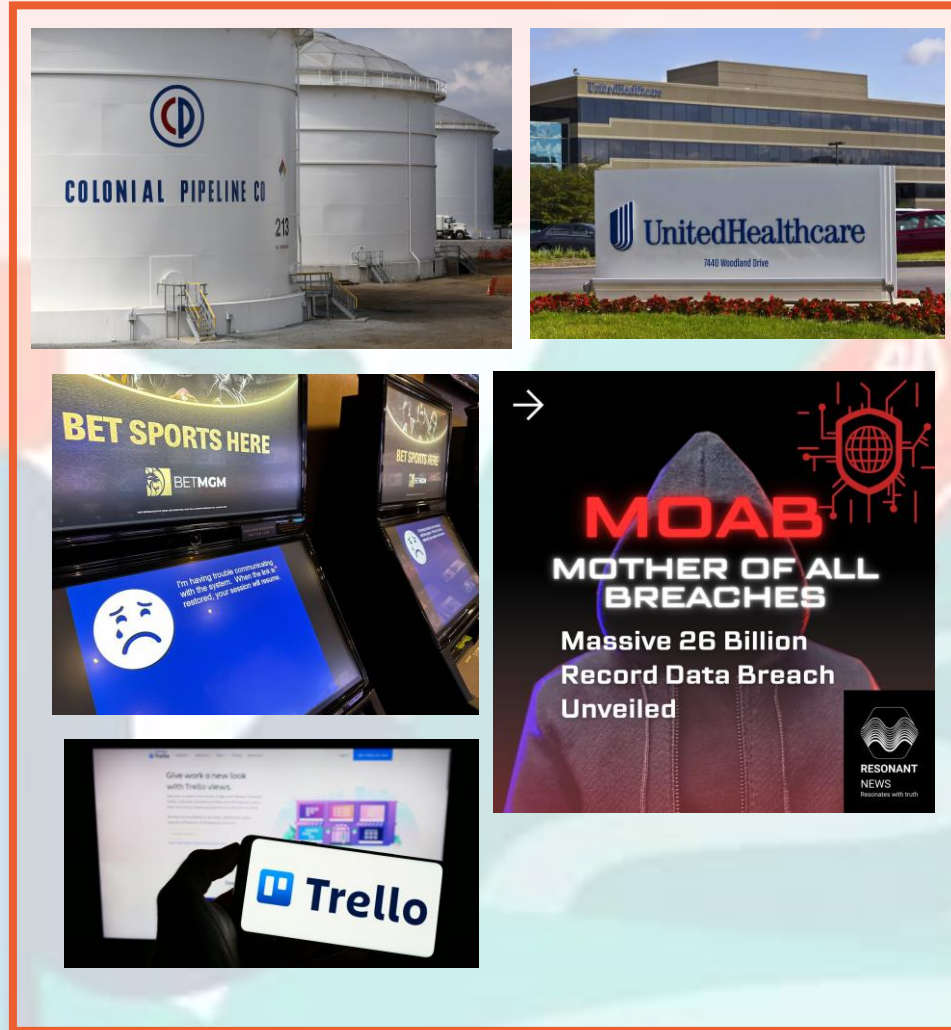


Why is Cybersecurity exciting?

Gadgets



News stories











Or Maybe the cool threat actor names?

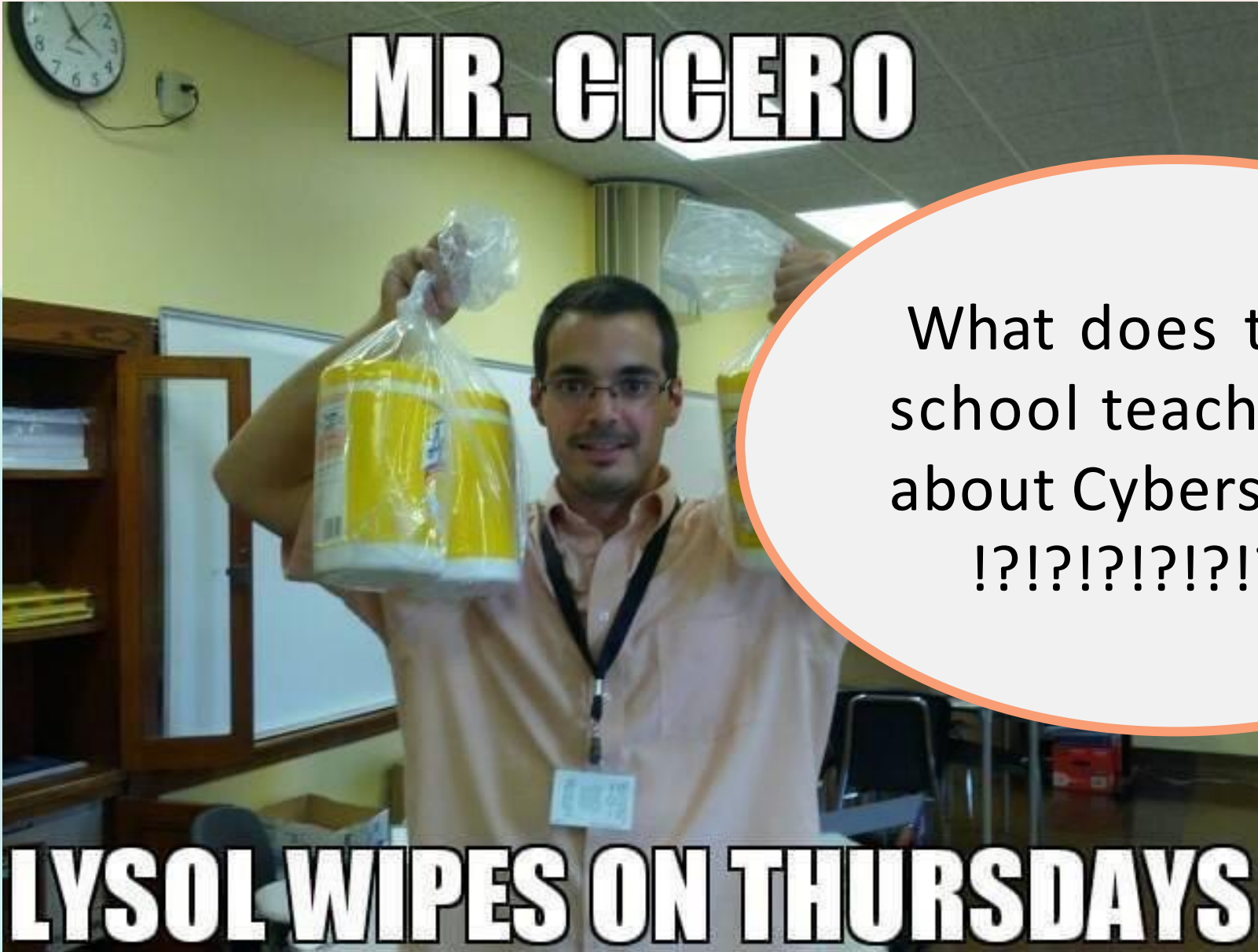
Octo Tempest

Peach Sandstorm

Onyx Sleet

Microsoft Naming Conventions:

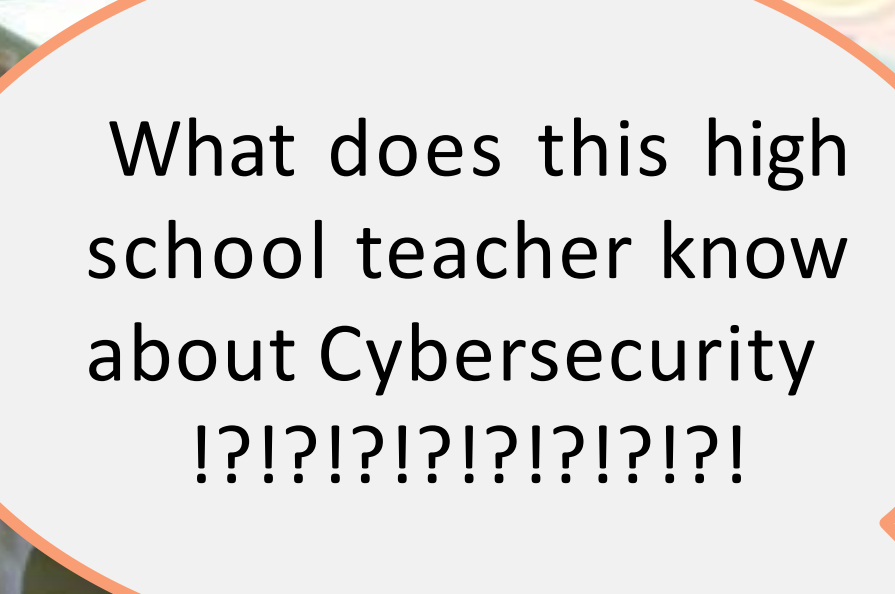
 Blizzard Russia	 Sleet North Korea	 Typhoon China
 Sandstorm Iran	 Storm Groups in development	 Tempest Financially motivated
 Tsunami Private sector offensive actor	 Flood Influence operations	

A man with glasses and a mustache, wearing a light-colored button-down shirt and a lanyard with an ID badge, stands in a classroom. He is holding up two large, yellow and white bottles of Lysol disinfectant. In the background, there is a clock on the wall, a whiteboard, and a wooden cabinet. The image is overlaid with text: 'MR. CIGERO' at the top, 'What does t school teach about Cybers !?!?!?!?!?' in a speech bubble on the right, and 'LYSOL WIPES ON THURSDAYS' at the bottom.

MR. CIGERO

What does t
school teach
about Cybers
!?!?!?!?!?

LYSOL WIPES ON THURSDAYS

A large, light blue speech bubble with a dark blue outline is centered on the slide. Inside the bubble, the text "What does this high school teacher know about Cybersecurity" is written in a large, black, sans-serif font. Below this, a series of ten question marks "!!!!!!!!!!" is displayed in a smaller, black, sans-serif font. The background of the slide is a blurred image of a classroom with students at their desks.

What does this high school teacher know about Cybersecurity
!!!!!!!!!!

A man with glasses and a mustache, wearing a light-colored button-down shirt and a lanyard with an ID badge, stands in a classroom. He is holding up two large, yellow-labeled bottles of Lysol disinfectant spray, one in each hand. The background shows a typical classroom environment with a whiteboard, a clock on the wall, and wooden shelves. A speech bubble on the right contains text about cyberbullying prevention. At the bottom, there is a large, bold caption.

MR. CIGERO

What does t
school teach
about Cybers
!?!?!?!?!?!?

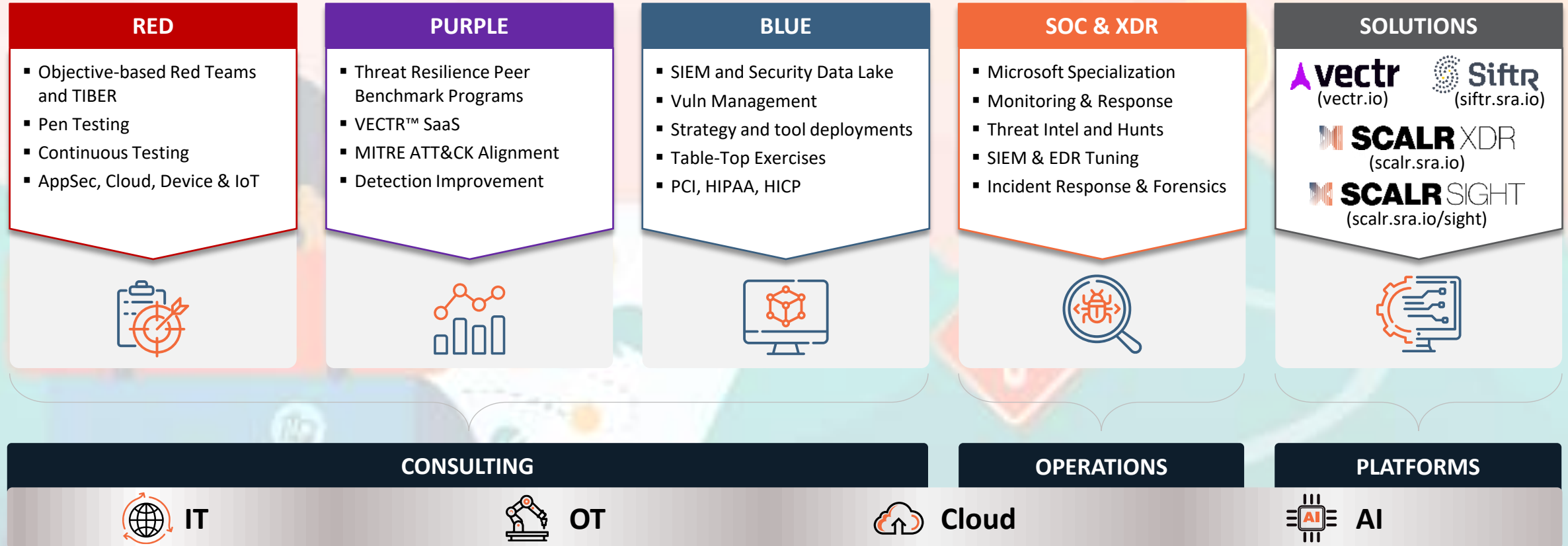
LYSOL WIPES ON THURSDAYS

My Journey



- AP World History Teacher @Rochester City School District
- Technology Specialist @Rochester City School District
- Edtech Consultant/Trainer/Deployment @Eduscape
- Technical Seller - Window EDU @Microsoft
- Program Manager – EDU Partner Ecosystem @Microsoft
- Product Manager – Defender Experts @Microsoft
- Service Delivery Manager @Microsoft
- Director of Strategic Alliances @SRA

What We Do



Helping you protect your business, your people, and your customers.

What is your goal?

- **Analyst:** Protects computer networks from cyber attacks by monitoring, investigating, and fixing security issues.
- **pen-tester:** Simulates attacks to test the security of computer systems, networks, applications and databases.
- **threat-hunter:** Proactively finds and stops advanced cyber threats that may evade security systems.
- **AI innovator:** Creates new AI models, algorithms, tools or frameworks for cyber defense, threat detection, incident response, risk assessment or vulnerability analysis.
- **Service Delivery Manager:** Manages the relationships with external security vendors and partners and monitors the performance and quality of the security services delivered to the clients.



Example Job #1

Job: Senior Security Engineer

Profession: Engineering

Location: Remote

BlueVoyant

Description: A SecEng will collaborate at the direction of the CISO to ensure that platform/product teams are aware of, and use, best practices for SecDevOps in delivery of their job functions. This will include building, maintaining and training on reference implementations for IaasCode instances (e.g., Hashicorp Vault, terraformed networking configurations, etc.). SecEng will also work with Software Engineering teams to ensure that the software delivery pipeline is as efficient and secure as possible using leading SecDevOps techniques.

Qualifications:

- Hands on experience using the AWS, GCP, and Azure console and CLI/SDK
- Mastery experience within AWS, GCP, and Azure
- Mastery experience with Linux + Windows Servers
- Mastery experience with Cloud Security
- Expertise implementing solutions in public cloud IaaS/PaaS
- Expertise in monitoring, administering, troubleshooting and identifying solutions in a cloud environment.
- Expertise in PKI Infrastructure
- Proficient experience with Hashicorp Tools
- Proficient experience with containerization platforms (Docker, Kubernetes, etc.)
- Proficient experience with Microsoft Applications
- Experience within cloud infrastructure including areas of sizing, provisioning, monitoring, and capacity management

Example Job #2

Job: Service Delivery Manager

Profession: Engineering

Location: Remote



Description: In this role you will work with an assigned set of customers and guide them throughout their managed service. You will represent Microsoft to them and constantly demonstrate the value we bring to the customer through weekly syncs, reports, and finding resolutions to their issues. At the same time, you will also have the duty to represent the customer to Microsoft and our product teams. If representing both Microsoft and our customers sounds interesting to you, please consider becoming a Solution Delivery Manager.

Qualifications:

- High-level of understanding of broad Security concepts, including Zero Trust, MITRE ATT&CK framework, and Secure-by-Design.
- Effective communication skills: adapting your style and level of information based on the audience
- Ability to forge strong relationships with customers (Business Decision Makers, CSOs and IT Leaders), communicating on behalf of Engineering, facilitating understanding of our value proposition and our services; direct experience working with customers
- An ability to work well within fast-paced, ambiguous situations where you need to define the problem, goal, solution and see it through to the end to deliver tangible outcomes
- Ability to meet Microsoft, customer and/or government security screening requirements are required for this role. These requirements include, but are not limited to the following specialized security screenings:
 - Microsoft Cloud Background Check: This position will be required to pass the Microsoft Cloud background check upon hire/transfer and every two years thereafter.

Example Job #3

Job: Cybersecurity Operations (CSOC) Consultant

Profession: Security Operations/Analyst

Location: Remote

Description: The Cybersecurity Operations Consultant position will be part of Security Risk Advisors' CyberSOC team. This role will be involved in the day-to-day, 24x7, operations of the SOC. This is an outstanding opportunity to work with a wide variety of tool sets and various client organizations.



Qualifications:

- Eyes on glass security monitoring for threats.
- Respond to alerts, investigate to determine if they are true positive or false positive.
- Use the latest security monitoring technologies to detect malware and hackers.
- Use Security Information Event Management tools (SIEM), Endpoint Detection & Response tools (EDR), and Network Security Monitoring tools (NSM) such as FireEye, Fidelis, Splunk, Intel/McAfee, RSA, IBM, Symantec, Resilient, Cybereason, Tanium, CarbonBlack, Bro and Snort.
- Thoroughly document work and present findings to management suitable for customer consumption.
- Attend conferences and training as required to maintain proficiency.
- Protect organization's value by keeping information confidential.
- Ability to work non-core hours, including weekends and night shifts.

Example Job #4



Job: Offensive Security Senior Consultant

Profession: Offensive Security / Pen-tester

Location: Rochester, NY

Description: The Offensive Security Senior Consultant position will be part of our Advisory practice on the Technical Assessments team. Our style of consulting is dynamic, innovative, fast-paced, and highly rewarding for both our clients and our team. This is an outstanding opportunity to work with a wide variety of tool sets and across various well-known client organizations.

Qualifications:

- Flexibility to accommodate changing schedules of client and project needs and willingness to work extended hours when needed.
- Demonstrable aptitude for technical writing, including assessment reports, presentations, and operating procedures.
- Experience communicating with clients and independently managing client projects.
- Knowledge of Windows and *NIX-based operating systems.
- Knowledge of networking fundamentals and common attacks/defenses.
- Experience managing multiple projects at once.
- Strong analytical skills with the ability to collect, organize, analyze, and disseminate significant amounts of information with attention to detail and accuracy.
- Strong written/verbal communication and interpersonal skills.
- Excellent technical skills, impeccable soft skills, and organization skills.
- Strong written and verbal communication skills to effectively communicate successes and obstacles with team members and leads, as well as client stakeholders.

How do we grow?

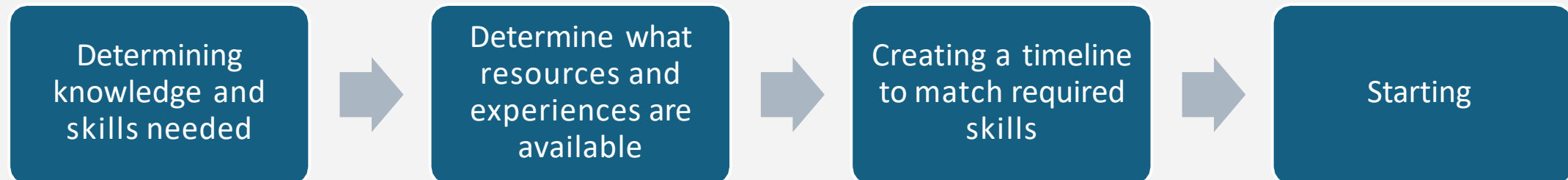
- Knowing the industry and options
- Understanding our transferable experience
- Setting a goal and/or target
- Determining gaps
- Creating action plan

Determining Next Steps

Skills & Knowledge Needed

— Transferable Knowledge & Skills

= Skills gap/Learning Opportunity



Beginning your Journey

News

- [Microsoft Security Blog](#)
- [SANS White Papers](#)
- [Google Security Blog](#)
- [Cybernews](#)
- [The Hacker News](#)

Product Agnostic Learning

- [UDEMY: Cyber Security Course for Beginners - Level 01](#)
- [Coursera: Introduction to Cyber Attacks](#)
- [Pluralsight: The Information Security Big Picture \(Free Trial\)](#)
- [Cybrary: Cybersecurity Foundations](#)
- [edX: Cybersecurity](#)

Product Learning/Certifications

- [Microsoft Security](#)
- [Palo Alto Networks](#)
- [AWS Security](#)
- [CrowdStrike](#)
- [Google](#)

Local Communities

- [ISC2 Chapters](#)
- [Cloud Security Alliance \(CSA\) Chapters](#)
- [Information Systems Security Association](#)
 - [Rochester ISSA](#)

Product Agnostic Certifications

- [CompTIA Security+](#)
- [GIAC](#)
- [CISSP](#)
- [CISA](#)
- [CISM](#)

Learning Labs

- [Hack the Box](#)
- [Try Hack Me](#)
- [Pentester Lab](#)

Creating Your Network

Regional Conferences

- [Find Local Bsides](#)
 - [BSidesROC - Saturday March 23, 2024](#)
 - [Bsides Buffalo – June 2024](#)
- [Regional Black Hat Events](#)
 - [SecTor – Black Hat](#)

National Conferences

- [Black Hat](#)
- [Blue Hat](#)
- [Def Con](#)
- [RSA Conference](#)

LinkedIn Groups

- [Canadian Cybersecurity Network](#)
- [Cyber Security](#)
- [CyberSecurity Community](#)

LinkedIn Contacts

- [Mike Pinch](#)
- [Joe Cicero \(me\)](#)
- [Tim Wainwright](#)
- [Mona Ghadiri @ Blue Voyant](#)
- [Ed Martin @ Microsoft](#)
- [Michael Melone @ Microsoft](#)
- [Abhishek Agrawal @ Microsoft](#)
- [Cordell BaanHofman @Red Canary](#)

Career Planning Template

Cybersecurity Career Planning Template

The Basics

Name:	
Cybersecurity Career Aspiration	
Timeframe:	<input type="checkbox"/> 3 Months <input type="checkbox"/> 6 Months <input type="checkbox"/> 9 Months <input type="checkbox"/> 12 Months
Your Potential Input Roles You Would Like to Explore:	<input type="checkbox"/> Goal Job 1 <input type="checkbox"/> Link to Job Post <input type="checkbox"/> Goal Job 2 <input type="checkbox"/> Link to Job Post <input type="checkbox"/> Goal Job 3 <input type="checkbox"/> Link to Job Post
List of Current Mentors & Colleagues:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Take Inventory

Skills/Qualifications Needed for Your Next Job:	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Your Top Skills/Qualifications as of Now:	<input type="checkbox"/> <input type="checkbox"/>

	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Growth Opportunities Regarding Skills/Qualifications on Cybersecurity:	Growth Area 1: <input type="checkbox"/> Resources Available to Grow: <input type="checkbox"/> Time to Achieve: Growth Area 2: <input type="checkbox"/> Resources Available to Grow: <input type="checkbox"/> Time to Achieve: Growth Area 3: <input type="checkbox"/> Resources Available to Grow: <input type="checkbox"/> Time to Achieve:
Your Communities and Group Memberships Regarding Cybersecurity:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Take Action	
Courses/Labs That will Help You Acquire Skills:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Experiences/Events to meet Cybersecurity Practitioners/influencers:	<ul style="list-style-type: none"> Local Groups: <ul style="list-style-type: none"> ○ ○ ○ Regional Conferences: <ul style="list-style-type: none"> ○ ○ ○ National Conferences <ul style="list-style-type: none"> ○ ○ ○
Increasing Social Network:	<input type="checkbox"/> Connect with Experts on LinkedIn

	<input type="checkbox"/> Schedule Informationals with people in cybersecurity with your ideal role <input type="checkbox"/> Join online/virtual communities
Demonstrate Ability	
Create Assets for the cybersecurity community:	<input type="checkbox"/> Create "how-to" videos (TikTok, Reels, YouTube) <input type="checkbox"/> Write blogs on a cybersecurity topic
Create visibility within the cybersecurity community:	<input type="checkbox"/> Re-post influencer content with your thoughts <input type="checkbox"/> Present at local/regional conferences <input type="checkbox"/> Attend cybersecurity meetups <input type="checkbox"/> Connect with hiring managers, recruiters
Apply for Multiple Jobs	
Apply for the job, over-and-over:	<input type="checkbox"/> Identify 20 interesting jobs <input type="checkbox"/> Connect with specific hiring managers/recruiters <input type="checkbox"/> Write job specific Resumes
Interviewing:	<input type="checkbox"/> Learn everything you can about the role and organization ahead of time <input type="checkbox"/> Schedule informationals with people on the hiring team <input type="checkbox"/> Create job specific talking points to reference during the interview <input type="checkbox"/> Cite clear examples with ample data to support

<https://github.com/joecicero/careercoaching>

Tips and Tricks to Shorten the Journey

- 
- An illustration of a person with dark hair, seen from the back, wearing a blue backpack with a red top section. The backpack has several icons on it: a graduation cap, a lightbulb, a star, and a shield. The person is holding a large white map with a dashed line path, a green leaf, and a yellow star. The background is a soft-focus landscape with green hills and a warm orange and pink sky with a yellow sun.
1. Develop a Strong Foundation
 2. Pursue Relevant Education and Certifications
 3. Learn About Cybersecurity Fundamentals
 4. Stay Informed
 5. Build Practical Skills
 6. Networking
 7. Create an Online Presence
 8. Specialize
 9. Soft Skills Matter
 10. Apply for Internships and Entry-Level Positions