About You

- Personal
    - Big Family
    - Sports
    - Food
        - Never missed a meal!
    - Travel
    - Community Service
    - Movies/Binge watching TV Shows
    - Love Learning new tech
        - Home automation/Building 1st PC
- My Background
    - Logic and Analytically minded person
    - I come from Mathematics and Statistics education
        - Taught and coached for several years
    - Cyber Security
        - Master's, Security+, Pluralsight courses
        - Exciting field
        - New challenges all the time

Why Arctic Wolf? And why I am most interested in this team at Arctic Wolf

Core Values: Diversity, Equity, Inclusion, and Belonging

1. Challenge
    - **Arctic Wolf's mission of taking ending cyber risk**
    - **challenge of how fast technology changes** > **threats changing**
    - I not only **love challenges** but I **thrive** on **challenges**
    - I will **protect people**.
2. Passion
    - Interested in Cyber security
        - 1. Fits my personality > Defender
            - Care and protect people
        - 2. Love learning
            - Read Cyber Security Hub Whitepapers
                - Help family have better password hygiene and complexity

        - 3. Personal experience
            - Situation: Social Engineering attack > ransomware
            - Task: Vulnerable > no choice > lost sense of security > no one else to go through it
            - Action: There has to be a way to prevent for me and others > initial interest
            - Result: Fed my fire > pursue education > in result that really fed my fire to educate myself on cyber security which led to getting a master's degree in cyber security, graduating in the top 3%, so that I could become that defender for others around me
3. Culture
    - Arctic Wolf **culture** of fostering and growing a diverse, equitable, and inclusive workplace where all feel safety and belonging.
    - be a **contributor** and bring my **creative** and **fun energy**
    - Help **protect** that **culture** by **respect** to those that **work** for **Arctic Wolf**

Interview Questions

—

What is the difference between Firewall, WAF, IPS, and IDS?

- **Firewall**
    - First line of defense
    - filters traffic from a source host to a destination host using TCP/UDP ports
    - establish rules
    - Next Gen firewalls that have more features (IDS, IPS)
- **Web Application Firewalls**
    - protect web servers from web exploits and HTTP attacks
- **Intrusion Detection System**
    - detects intrusions on a server or application
    - sends an alert about the intrusion in real time
    - searches for attack signatures or traffic patterns
        - SNORT IPS/IDS open source packet sniffer
            - Decoder - processes captured packets, identifies protocol
            - Detection Engine - does the intrusion detection, checks against rules and actions
            - Log - each rule has specific logging and alert
        - Suricata
            - supports multithreading

        - More than one user at a time w/o multiple copies running
- **Intrusion Prevention System**
    - inspects traffic after a firewall
    - detects and prevents malicious traffic
    - inline with the data path
    - this can cause decreased network performance
- **EDR**
    - Monitors endpoints to mitigate threats
    - Similar to AntiVirus
        - Hash Values of IoC's
    - Monitors for malicious activity and behaviors
    - XDR > collects data from multiple security layers (email, endpoint, server, cloud)
        - Faster detection and response times
- **Network Configuration**
    - Firewall first
        - DMZ
    - MDF, core switch, servers
    - IDF, network switches
    - Wireless access point, workstations, phones VoIP
- **Acknowledge Business Feasibility**
    - Budget
    - Dealing with Legacy Systems
    - Quantitative (knowledge/experience) and Qualitative (measurable data) Risk
        - Risk Appetite
- **Group Policy Objects**
    - Collection of policy settings
        - Passwords
        - Software
        - Golden Image
            - Baseline GPO for user vs admin
            - CIS benchmark for GPO
- **Recent Vulnerability**
    - Uber in Sept
        - Internal servers got accessed
            - elevated permission
            - Defaced internal site
        - Contractor personal device had malware
            - Stole credentials

        - MFA fatigue
            - Multiple requests until they accepted
    - Disabled compromised accounts
- **Malware Customer Call**
    - Ask questions
        - Look for IoC's
            - Spreading to other systems > ransomware
            - Phoning home
                - Command and control
        - They may not know what they are talking about

MITRE ATT&CK Framework

- It is a library database from real-world observations of tactics and techniques that adversaries use
- Foundation for the development of specific threat models throughout the cybersecurity community
- Covers topics like Reconnaissance, Privilege Escalation, Lateral Movement
    - Explains what adversary is doing
    - How to Mitigate with controls
    - How to detect
- Scanning
    - Vulnerability Scanning
        - Check for configuration of apps/software of target
        - Info used to identify known exploitable vulnerabilities
    - Detection
        - Use IPS/IDS to analyze network traffic for patterns of IoC's
    - Mitigation
        - Harden network devices
            - Configure Firewall
            - Secure remote access points
            - Block unused/unneeded ports
        - Perform vulnerability scans and pen tests to find security holes
        - Software Patching Schedule

Active Directory

- Database and set of services
    - connect users with the network resources to do their job
    - Info about environment
        - Users
        - Computers
            - Who's allowed to do what through **Least Privilege**

You’re a brand new CISO of a small company and want to secure your endpoints. What is your first step?

- 1st: Discover
    - Discover all devices connected to company network
    - Monitor new connections, especially unknown device connections
- 2nd: Inventory
    - Take inventory of
        - OS, firmware, software versions running
        - Prioritize known vulnerabilities
        - Create patch schedule
- 3rd: Monitor
    - Monitor endpoints, files, network for changes
    - Look for IoC’s, policy violations
    - Determine severity
- 4th: Protect
    - Deploy advanced and automated endpoint protection EDR
    - This should work in tandem with SEIM

Irate Customer

- 3 Touch Points
    - 1. Listen > Show it through notes > invested in conversation
    - 2. Check for Understanding > repeat back to them > Validate concerns
    - 3. Take Action > short term > long term

OWASP Top 10

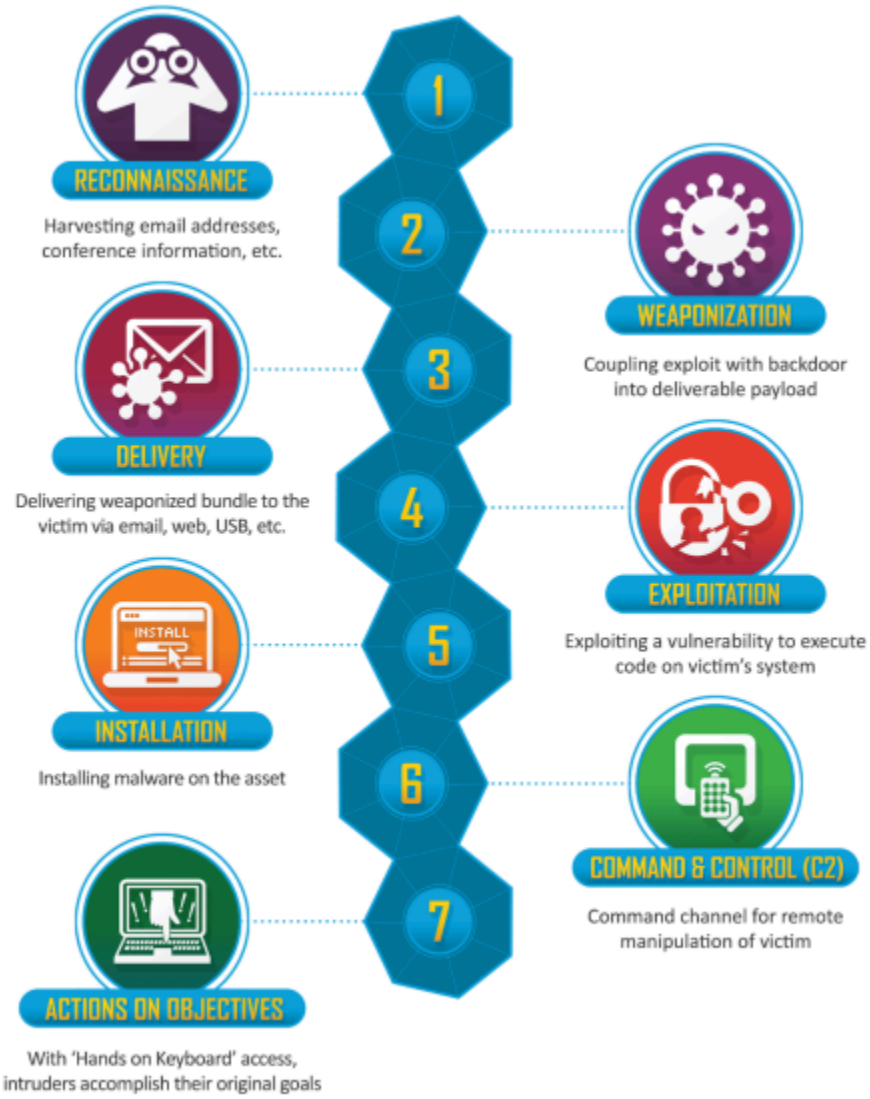
- Document for awareness for developers and web app security
- Most critical security risks
- 1st step towards secure coding

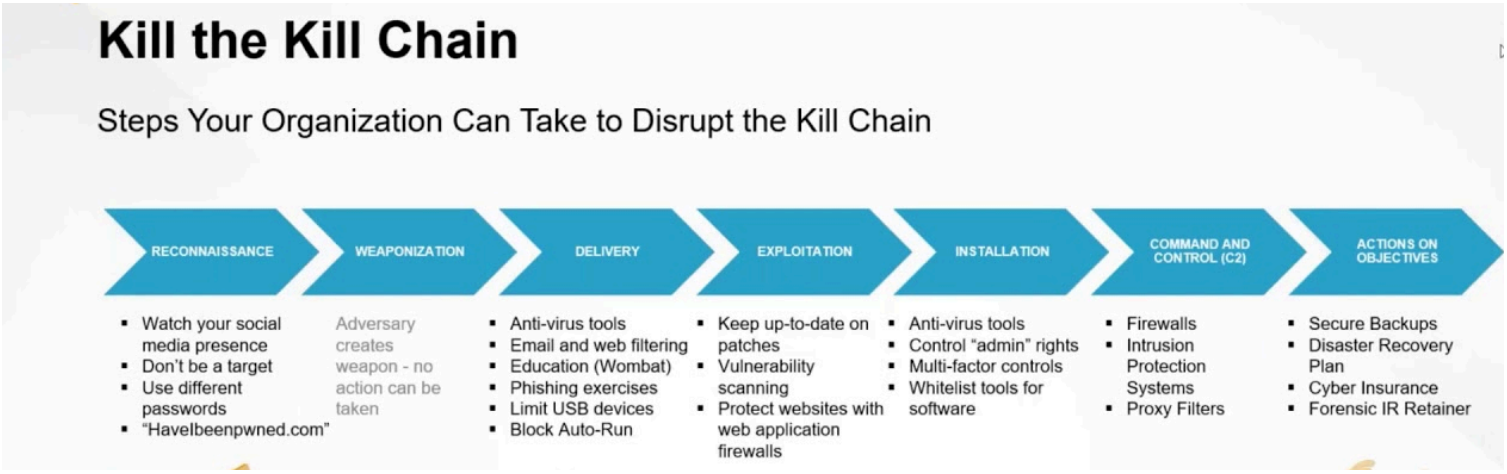
Email

- DMARC
    - Standard email authentication method
        - Helps prevent spoofing organization domain
- DKIM

- Authentication method
- Detects forged sender addresses
    - Receiver can check if email was sent by authorized owner of domain
- SPF
    - Standard email authentication
    - Helps against spoofing
        - Your emails don’t get marked spam

Cyber Kill Chain





We expect you to "fail" when you're new. Describe a time when you failed and what you did after.

Situation:

- Mathematics and Statistics teacher
    - College level course
- Students struggling with course material
    - Has been worst performing math class for years 15% pass rate
    - Low enrollment 15 students
        - 1st year 20%
        - Considered dropping course from school
        - Told admin that I could make it better

Task:

- Establish an improved methodology of instruction to improve comprehension, pass rate
- Recruit students for next year

Action:

- Contacted teachers district/state
    - Trusted, new they were successful
    - Scheduled observations and requested assessment data
- Analyzed data with statistics software
- established a correlation coefficient for highest outcome
    - No need to reinvent the wheel, but can be made better
- Implemented a new methodology

Result:

- Saw an increase of pass rate to 57% first year
- Wasn't satisfied, knew it could be even better

- combination with my own creative ideas
    - 2nd year growth to 83% second year
    - Add 2 periods to accommodate 115 students for year 3

Lack of Experience

- My cyber experience has always started as a disadvantage
- Master's Program with analytical and logic based background
    - Knew I was at a disadvantage from other students
        - Needed to overcome that
    - I wanted to get to their level, then be a leader
    - In order to do that I needed to work harder
    - Graduate top of class
- Entering Industry
    - Know I am at a disadvantage
    - I have experience overcoming that
        - Hard work and determination

PCI Experience

Core Value: Creativity and Fun

Situation: I worked on a project for Dental practice that just opened and didn't have any security policies and procedures in effect.

Task: Establish measures to ensure the **physical** and **technical security** along with any **requirements** of **regulatory bodies**.

Action: I **Rearched, Designed,** and made a **plan of action** for the establishment of **security** measures based on **industry best practices**. These measures included **physical** and **technical security policies** and procedures ranging from **alarm monitoring system** and **medication access management** to **IAM** and **training/awareness** requirements. In the research it was discovered that there are **two compliance organizations** that the dental practice falls under, **HIPAA** and **PCI**.

Result: The dental practice was able to have a **robust plan** to secure both their **physical** and **technical environment** from security breaches. Established relationship with an **acquiring bank** (Wells Fargo) along with **POS**

devices and set forth detailed plans to cover the **12 areas** of the **PCI DSS** compliance requirements along with recommendations of having a Qualified Security Assessor (**QSA**) audit their practice to ensure compliance.

Phishing Email Campaign

Core Value: Empathy “we care for people, so they can be their best”

Situation: I worked on a team project to conduct an **organization wide phishing awareness** and **training campaign**

Task: My team was tasked to Develop a method to **reduce** the **likelihood** of a breach due to a **phishing attack**.

Action: I **Researched** common **phishing methods** over different avenues (**email**, **sms**, etc.) and found recommendations from industry professionals from reading **white pages** from a cyber security online **community** (techtarget/info security group) and the “11 Commandments of Running a Phishing Campaign”

Result: I was able to Develop a Phishing Campaign plan that included a **fun interactive** and incentive-based training to “**gamify**” the training with a Jeopardy theme. I also made a **landing page** that focuses on **teaching employees**, **not blaming** them, and having **empathy** through **positive messages** to encourage the right **mindset**, as well as a plan to include **senior management**.

Common Identifiers
Strange Greetings, Grammar Errors, Sense of Urgency, Abnormalities in Email Addresses

Why PCI?

Core Value: Respect
Situation: I am very much a **rules guy.** I love when things are **organized** and have **structure**.

Task: Throughout my master’s program I was exposed to **many different career paths** that are available in cyber security and I knew I needed to find something that **fits the type of person** that I am. I took a course all about **GRC** and learned a lot about NIST, ISO, HIPAA, SOX, and PCI. **PCI really fascinated me** but we didn’t get to spend a lot of time on it since there was so much to cover.

Action: I knew I wanted to **learn more** about PCI so I **met with my professor** and he was able to get me access to **Pluralsight** so I could take some **online courses**.

Result: I **finished a course and have just started another one that prepares for the PCIP exam**. I've really loved what I have learned and researched and know this is perfect for me.

Lack of Experience

Core Value: Humility

I feel that I have a great **advantage** to this position because I have a **natural ability and excitement for continuous learning and growth** which as you know, is **essential** in a world of **advancing technology**, for example:

Situation: When I began my masters program, I was surrounded by many **professionals** that already had **years of experience in IT**. I knew that I had a **lot to learn** and knew that I had to **work even harder** to excel in the program and field.

Task: I knew I needed to **learn complex materia**l and be able to **apply it quickly**

Action: I established a regimen for coursework in order to ensure that all the timelines were met. I took the initiative in leading team projects with members of diverse IT backgrounds, through assigning roles, scheduling check points and reviews, final oversight of project quality, and accuracy of deliverables. I also sought out opportunities to collaborate with professors and other peers to gain their perspectives through their industry experience.

Result: In result, through all my hard work and dedication, I was able to complete my program, outperforming even those who had prior background and experience in the field, in the top 3% of my graduating class with a 3.97 GPA. In this world of advancing technology, having someone who is proactive in continuous learning and growth, as well as adaptable to changes in security practices would be an ideal asset and I assure you that I am that person.

My Questions:

1. Rachel, since you have been there a while, What were some of your favorite things when you first started at hyatt? What about today? What are some of the areas you feel like need to improve?

2. Jon, coming from a background in law enforcement, it sounds like you have been a protector in various ways, what is your why for choosing cyber security?

3. I love Arctic Wolf's **Core Values: Diversity, Equity, Inclusion, and Belonging**- What are some recent things that Hyatt has done to reiterate these values to this team?

4. For you personally what was one challenge you faced and how did you overcome that?

5. For you and your family, what is your opinion on the work/life balance?

6. I am very big on learning and continuous growth of skills and knowledge. Does Arctic Wolf offer any programs or support for employees to stay relevant in cyber security by attend workshops, conferences, or acquire certifications?

Technical Domain	**Questions (interactive or not)**
IDS/IPS	· What are some ways to detect attacks on a network level? · Have you ever used an IDS/IPS · How does an IPS/IDS work/ what does it do? · How do you determine how a snort/Suricata rule flagged?
Endpoint	· What endpoint detection or security products are you familiar with? · How have you used this product on a regular basis, if so, what for?
Perimeter	· How would you harden/protect a public facing Web Server? · Are you familiar with hardening IIS or WordPress? o If so, what ways can you help harden these systems? · What is a DMZ, and how is it used?

Networking	1. Build a complex network (Interactive) 2. What happens when you type "http://google.com " into a brand new computer? 3. How would you troubleshoot a host that is unable to connect to the internet?
SIEM	· Have you used a SIEM before? o If so, what for, and what kind of example investigations did you perform?
Security Fundamentals	1. Describe defense in depth (or layered security). What does that look like in the network you created earlier? 2. Walk through your thought process in examining an event or alert that appears malicious provided by a network sensor? 3. Describe how you would investigate a malware infection or C&C traffic on a workstation in your environment? 4. How would you investigate a URL that a customer is saying is malicious?
Cloud (IaaS/PaaS)	· What sort of behaviors would you look for to determine whether or not an EC2/VM may be compromised?
Public Key Infrastructure and Key Management	· What security recommendations would you give for an on-prem PKI environment? (AD Certificate Services). Why?
Cloud (SaaS)	· What sort of behavior would tell you that an Office 365 account has been compromised?

	· What methods could you use to help harden access to Azure/Office 365/AWS/GCP?
Risk & Compliance (Vulnerability Assessment and Scanning)	1. How would you prioritize risks for a patch management program? 2. What strategies would you employ to get an organization through a compliance audit? 3. You run an external scan on the environment and determine port 80, 443, 445 and 3389 are all open to the internet. What are those ports? Do any concern you? What would you do about it? 4. What are some of the challenges or risks of running vulnerability scanning within an internet network?
Windows Server	· Have you ever used Windows Server? · What is group policy and how is it used? · Have you ever configured syslog forwarding?

E-mail	· Can you tell us the differences between DMARC/DKIM/SPF/ARC? o https://support.google.com/a/topic/9061731?hl=en&ref_topic=7556782 o SPF is a DNS record that allows the owner of a domain to specify which mail servers they use to send email from that domain. § Policy can report only, block reject non-authorized mail servers or do nothing. o DKIM is a form of email authentication that validates the sender to the recipient mail gateway. (Combination of DNS record and public/private key in the mail server/gateway) o DMARC is a DNS record policy that gives instructions to the recipient mail gateway on what to do if policy matches or mismatch with the DMARC instructions. § Reject, send to junk-folder, report-only or do nothing. o ARC (Authenticated Received Chain) § Preserve the DKIM into intermediaries authorized mail relays (e.g.: O365 → Mimecast → Zendesk → end recipient)
Complexity of Work	· What was one of your most difficult issues you've dealt with at work, and how did you solve it? o Describe a security issue or crisis that you resolved.
Successes	· Tell us of a story where you provided significant value to your organization.
Other	· What is a skill you bring that you might consider a differentiator between you and other applicants?

(Python, documentation, etc)	· What has been your favorite technical project at home or at work?
Move to technical assessment	1. Can you name two or three security vulnerabilities as per Open Web Application Security Project (OWASP)? 2. Can you name one or more phases of the Cyber Kill Chain? 3. Have you used MITRE before? 1. Describe how you would MITRE ATT&CK could help an organization?