Critical Insight®

WEBINAR

What ChatGPT Won’t Tell You About Virtual Chief Information Security Officers (vCISO)

Things to Know

- Livestorm begins all webinars with your sound on mute. If you can't hear us, click on the screen to turn on the sound.
- Your microphone will remain muted, but please use the chat to talk to us!
- If the alerts are too much, you can mute them by clicking the bell (on the right).
- You will automatically get a recording but if you want the presentation slides, email ellie.miller@criticalinsight.com

Today's Speakers

Michael Hamilton

Critical Insight Founder, CISO, and Former CISO of Seattle

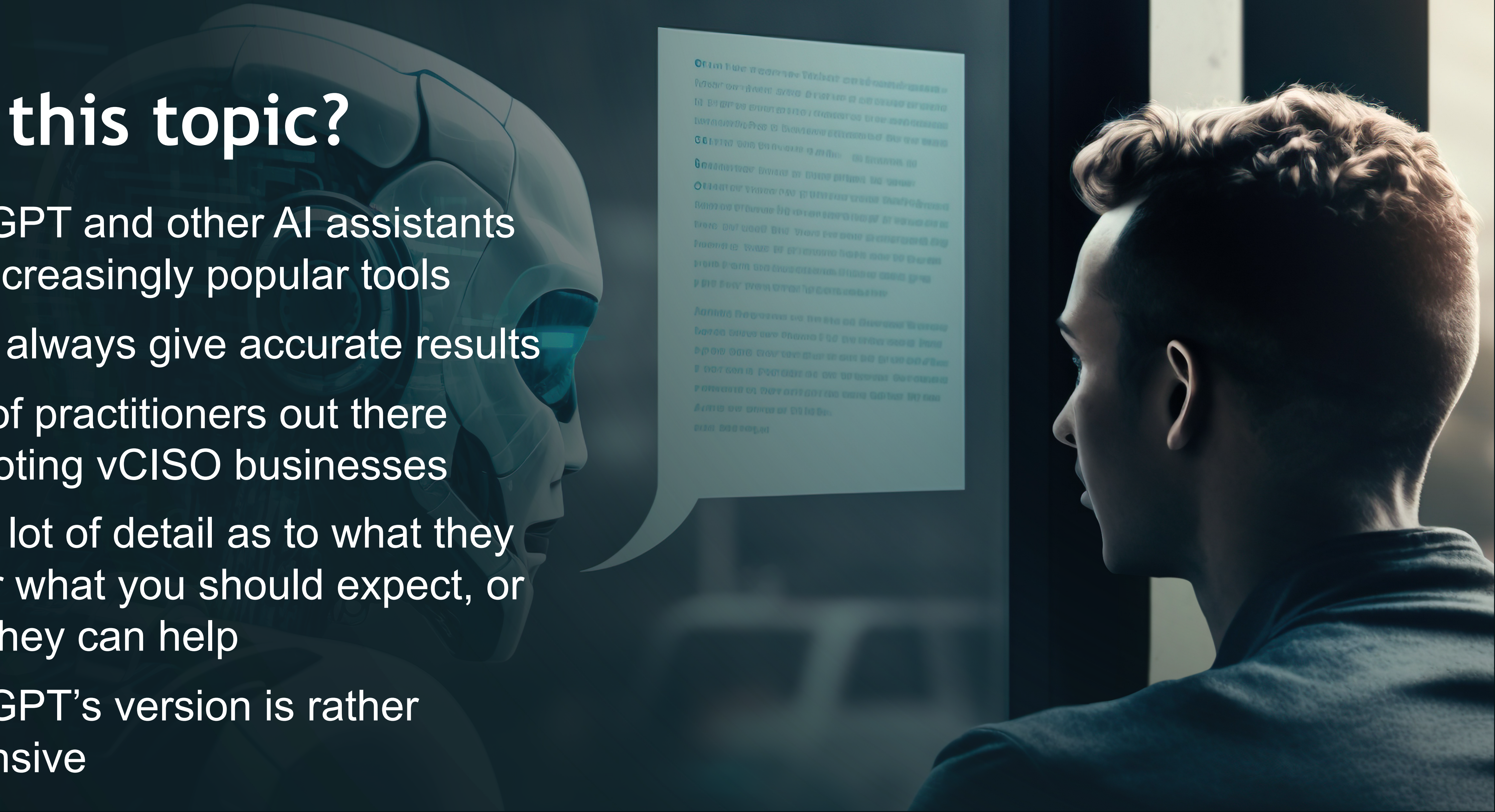
Brad Swanson

Critical Insight vCISO

Critical Insight®

Why this topic?

- ChatGPT and other AI assistants are increasingly popular tools
- Don’t always give accurate results
- Lots of practitioners out there promoting vCISO businesses
- Not a lot of detail as to what they do, or what you should expect, or how they can help
- ChatGPT’s version is rather expansive



What ChatGPT Will Tell You:

Prompt: What should be expected of a virtual CISO?

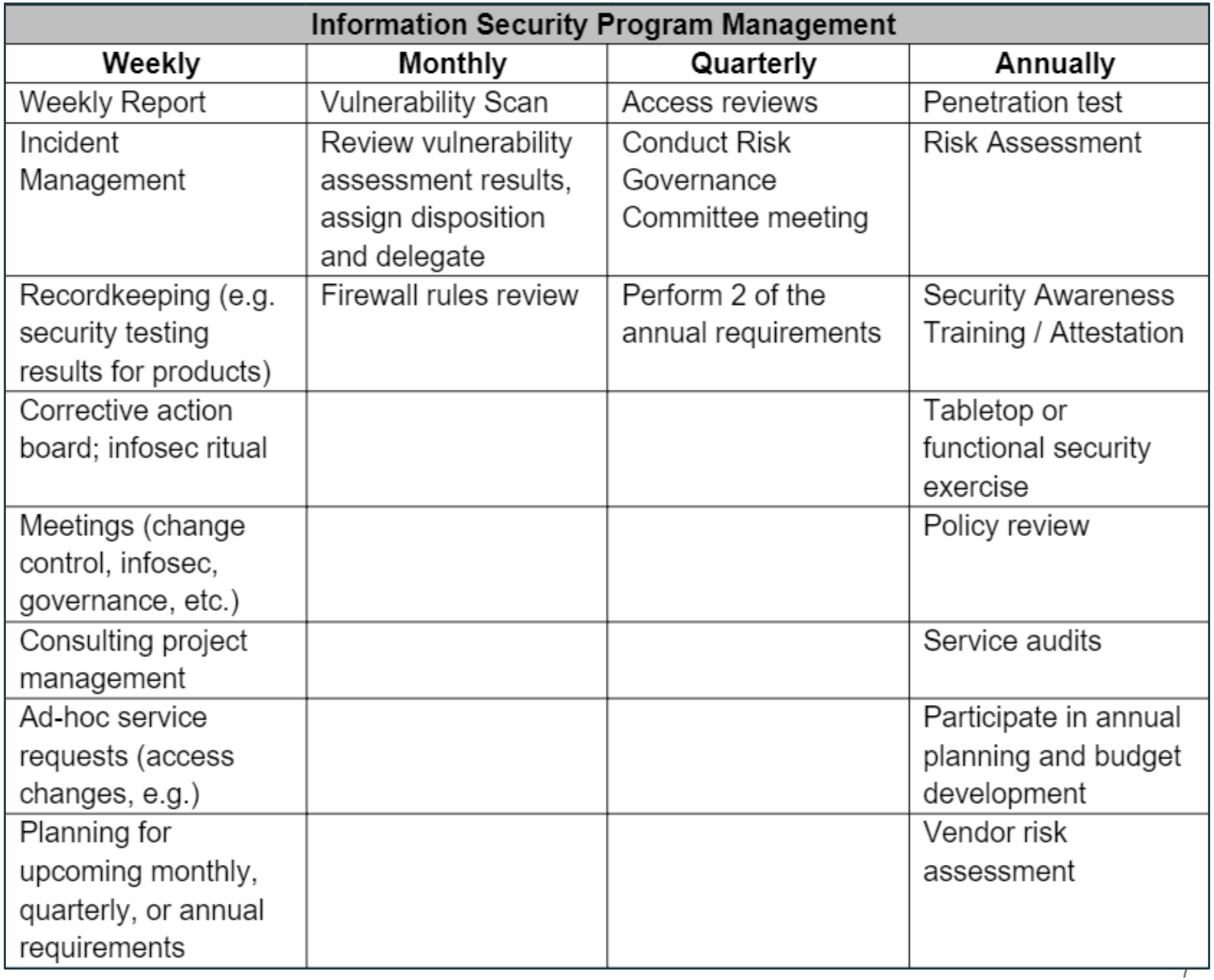
1. Cybersecurity Strategy Development
2. Risk Assessment and Management
3. Compliance and Regulatory Adherence
4. Security Infrastructure Planning and Implementation
5. Security Incident Response
6. Training and Awareness
7. Vendor Risk Management
8. Continuous Monitoring and Improvement
9. Board and Executive Reporting
10. Flexibility and Availability

We Say That’s Expansive Because…

- That’s an entire information security program
- A V-CISO alone is not an entire team
- Those tasks are for a company with a lot of security maturity
- Not all those tasks are relevant to every sector
- Every organization’s needs are unique, and one size doesn’t fit all for cybersecurity

All The Things

- You may not need assistance for all these tasks
- You may not be regulated or audited, just trying to meet insurance requirements
- Your Board, Commission, or Council may want advisory services only



Information Security Program Management			
Weekly	**Monthly**	**Quarterly**	**Annually**
Weekly Report	Vulnerability Scan	Access reviews	Penetration test
Incident Management	Review vulnerability assessment results, assign disposition and delegate	Conduct Risk Governance Committee meeting	Risk Assessment
Recordkeeping (e.g. security testing results for products)	Firewall rules review	Perform 2 of the annual requirements	Security Awareness Training / Attestation
Corrective action board; infosec ritual			Tabletop or functional security exercise
Meetings (change control, infosec, governance, etc.)			Policy review
Consulting project management			Service audits
Ad-hoc service requests (access changes, e.g.)			Participate in annual planning and budget development
Planning for upcoming monthly, quarterly, or annual requirements			Vendor risk assessment

Let's Simplify

Critical Insight

Reasons For Outsourcing This Role

- Increasing regulation uniformly calling for improvements in governance
  - Risk governance and Executive participation in risk management
  - Cybersecurity representation to the Board of Directors
- Third-party risk management is calling on you to “show your papers”
- Candidates are in short supply
  - Need sector-specific experience
  - Cost
- You may not need a full-time position filled

Strategic Planning

1. Develop rituals – standing meetings with cybersecurity team and/or network/desktop/server teams
2. Create a risk governance committee for adjudicating identified risks
3. Conduct a risk assessment or evaluate efforts that are recent
4. Assign a disposition to each identified risk
5. Run results through the risk governance committee for concurrence
6. Develop a corrective action roadmap
7. Use rituals to pass risks and vulnerabilities for resolution
8. Track and report on progress

Developing those recurring rituals to integrate with the existing team and resources is extremely important for success.

Compliance and Oversight

1. Understand what regulatory requirements apply
   - HIPAA, PCI-DSS, CJIS, NERC-CIP, CMMC, NIST 800-171
2. Evaluate insurance requirements
3. Cross-walk previous risk assessment with other requirements
4. Denote which tasks are outstanding and schedule them
5. Review artifact collection and storage
6. Assist with audit(s) and/or develop materials for distribution

YES, your V-CISO may be *performing* some of these tasks as well as *designing* and *delegating* them, for example policy review, third party risk management, etc.

Education and Advocacy

1. Create security metrics reporting for Executives; deliver to risk governance committee
2. Based on sector and threat model, develop messaging for company personas
   - Users, Administrators, Executives and Board
3. Integrate messaging with existing LMS or service OR develop content; optionally deliver
4. Create materials to be included in Board of Directors meetings
5. Provide information on new threats, risk trends, legal and regulatory risk

Act as a strategic advisor to the business, using business language. Use examples from other organizations in the sector.

Critical Insight®

Client Responsibilities

What a Virtual CISO Needs from you

Client Responsibilities

- Ensure adequate security budget
- Provide security staff management
- Maintain external contract/relationship
- Understand overall company security risks and accountability model
- Conduct operational security tasks (e.g., Admin and operation of security tools, firewalls, etc.)
- Provide the point of contact for internal company relationships

Without Executive commitment and support, it is unlikely that a V-CISO practitioner would take on the engagement

Choose Carefully

- Virtual CISOs lack company- or sector-specific knowledge
- They are temporary, but you want a durable outcome
- They may not integrate well with IT teams
- Some have held onto 'old battles' and not knowledgeable on current threats
- Not all experience is relevant – do they know what you need them to know?

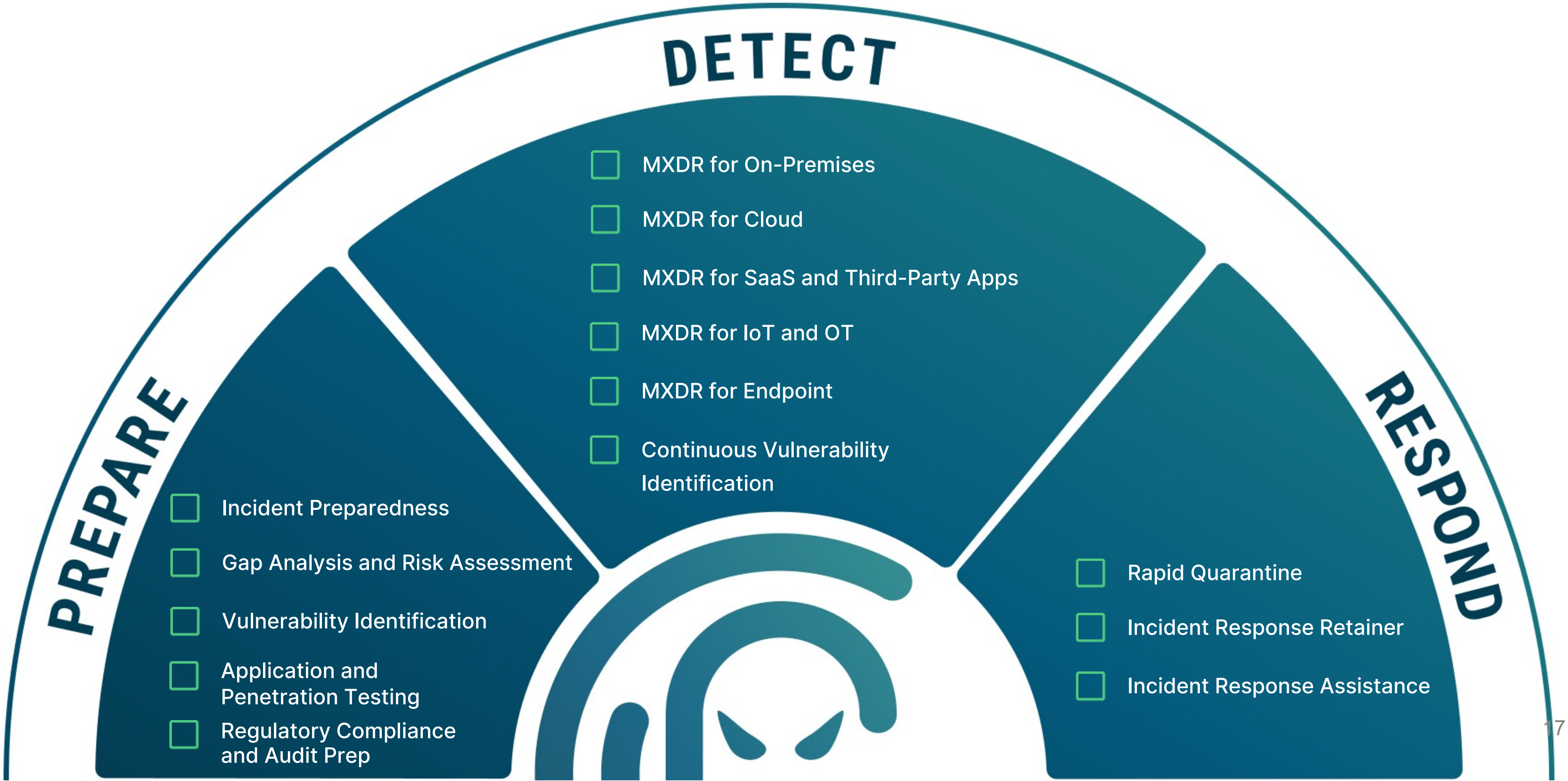
Finally, Some Hiring/Interviewing Tips

1. Has the candidate ever been the CISO in an organization?
   - Can include CISO, previous V-CISO, leadership/management
2. Does the candidate have experience in your sector?
3. Does the candidate have good communication skills?
   - Must include executive-level business communication
   - Should provide you a writing sample
4. Can the candidate speak to your specific regulatory requirements?
5. Has the candidate ever taken an organization through an audit?

Critical Insight®

Questions?

Cybersecurity-as-a-Service



PREPARE

- □ Incident Preparedness
- □ Gap Analysis and Risk Assessment
- □ Vulnerability Identification
- □ Application and Penetration Testing
- □ Regulatory Compliance and Audit Prep

DETECT

- □ MXDR for On-Premises
- □ MXDR for Cloud
- □ MXDR for SaaS and Third-Party Apps
- □ MXDR for IoT and OT
- □ MXDR for Endpoint
- □ Continuous Vulnerability Identification

RESPOND

- □ Rapid Quarantine
- □ Incident Response Retainer
- □ Incident Response Assistance

Stay Connected

- Sign up for:
  - Daily IT Security News Blast – Curated by Mike Hamilton for the last 15 years
  - Free monthly security awareness trainings online
  - Regular online urgent panel webinars and podcasts
  - More about PISCES: www.pisces-intl.org

Critical Insight®

Thanks for joining

Questions?

Mike.hamilton@criticalinsight.com

Ellie.miller@criticalinsight.com