25 Reasons why Military Veterans are Ready-Made for Cybersecurity Careers

LESTER CHNG

PART 2
20 OUT OF 25

11/25

Organizational Ability

The veteran has experience and expertise in organizing projects, exercises, and operations

- detailed phases of operations
- hour by hours training programs
- management across various teams

Effective project management in cybersecurity

- security tools have to be deployed
- metrics, kpi, and data have to be tracked

These are second nature tasks for veterans

Organizational Ability	

12/25

Understanding Enemy

Cyber warfare has an enemy

- In order to defend/attack assets, we need to understand the enemy
  - capabilities
  - tactics
  - objectives

Warfare in cybersecurity

- the direct application to this is cyber threat intelligence and the profiling of threat actors
- military concepts are used in cyber threat intelligence to make the best assessments

13/25

Understanding Strategy

Veterans are ingrained with understanding an overarching strategy of a campaign

- drives prioritization
- operational plans
- lays foundation for tactical plans

Strategy in Cybersecurity

- there are multiple tools, vulnerabilities, teams to build to structure an effective cybersecurity organization
- a holistic strategy is required to drive efficiencies and effectiveness

Understanding Strategy

Understanding Systems

The military operates in a system-in-system structure

- collaboration and coordination is vital
- systems thinking across layers
- understanding impact of changes

Systems in cybersecurity

- cybersecurity tools and changes impact multiple stakeholders
- managing these implementations as a system is vital to maintain integrity

15/25

Understanding Concepts

Veterans apply military concepts in their planning and execution

- defense in depth
- deception
- disinformation

Concepts in cybersecurity

- direct application to threat assessments and cyber defence concepts
- layered defense, hardening, honeypots, operational resilience, risk assessment

Understanding Concepts

16/25

Flexibility and Adaptability

Military veterans plan in extreme detail but are also highly adaptable to changing circumstances

- high situation awareness
- keen sense of changing information
- "war is the mother of invention"

Adaptability in cybersecurity

- mangement of multiple stakeholders to adhere to standards, implement tools, and articulation of risk
- it is not my way or the highway
- your program will fail if you are not flexible

Flexibility and Adaptability	

17/25

Understanding Intelligence

Intelligence drives decision and actions

- intelligence preparation of the battlespace
- daily intelligence briefs, requests of information, intelligence requirements
- sense-making of information

Intelligence in Cybersecurity

- the intelligence structure in cybersecurity has its roots from military intelligence
- corporate leaders need to quickly learn that in cyber warfare, information is a premium and decisions have to be made with best known intelligence [usually scanty at best]

18/25

Standards and Competency

The military loves standards and competency means life or death

- adherence to rules, regulations are drilled from day 1
- competency in your vocation is a given

Standards and Competency in cybersecurity

- security standards are critical in maintaining overall posture
- discipline in maintaining competency of skill and knowledge are vital especially in DFIR (digital forensics and incident response)

Standards and Competency

19/25

Understanding Vulnerabilities

Military operational plans constantly assess vulnerabilities

- reinforce your weakest flanks
- enhance surveillance in that space
- misinformation and deception tactics

Vulnerabilities in Cybersecurity

- not just the "traditional" vuln management
- assessment of blind spots, shadow IT
- gaps of current security tools
- mitigation measures

20/25

Understanding Crisis Management

Military veterans understand crisis intimately

- concepts such as establishing a battle rhythm, crisis response, early warning, shaping the narrative, coordination of assets

Crisis Management in Cybersecurity

- cyber attacks impact multiple teams and the coordination of response requires various stakeholders
- accuracy of information, cadence of reporting, roles and responsibilities, decision authorization are part of the response

Understanding Crisis Management

STAY TUNED FOR PART 3

Connect with me on LinkedIn

Ring the notification bell to know when I post

@Lester Chng