NEXT PEAK

Cyber Operational Augmentation

Our Proposition

The Challenge:

- Companies in all industries globally are struggling to attract and retain top-level cyber talent, particularly in leadership roles
    - Over 60,000 unfilled cybersecurity positions in the US
- Market competition increases barriers for small and medium companies that may lack the resources to afford full-time cybersecurity leadership
- Larger companies may also face challenges replacing cyber leaders and cyber talent transitioning out of roles due to high turnover in the field
- Workforce challenges are closely interrelated with cyber risk, with understaffed organizations reporting higher levels of intrusions

We Provide:

- Next Peak offers flexible cybersecurity talent, leadership and staff augmentation to match client's needs for the short to medium term
- We can provide highly experienced talent over a limited period in areas such as:
    - **Virtual CISO**
    - **Security Engineering & Operations**
    - **Cyber Governance and Risk**
    - **Cyber Exercises**
- Our operational augmentation engagements enhance the foundations of cyber programs and ensure operational measures are implemented to mitigate critical business risks
- Next Peak talent draws from world-class network of cyber defenders who have set up systems. run operations and exercises in military, government and multinational corporate settings

Next Peak Overview

Our Leadership Team

- Drove White House cybersecurity strategy & programs
- Commanded the US Air Force's cyber warfare capabilities
- Led one of the largest global corporate cyber uplifts
- Designed and led multiple security operations centers as well as national, military & corporate exercise programs
- Pioneered Advanced Persistent Threat (APT) & Operational Collaboration concepts

Greg Rattray, Ph D.
Colonel, USAF, (Ret)
Partner/Co-Founder

Jim Cummings
Colonel, USAF, (Ret)
Partner/Co-Founder

Collaboration Partners

Cyber Workforce Challenges

Cyber Talent is Scarce

- In the US, there are over 90,000 CISSPs, yet over 106,000 job openings requiring the certification
- Over 60% of enterprises say they have unfilled cybersecurity positions in March 2022, up 8% since 2021
- InfoSec roles anticipated to grow by +30% in next 5 years
- Global cyber workforce would need to grow 65% to meet demand
- On trajectory for over 3 million open positions globally in 2025

Recruitment is Competitive

- Attracting and retaining top cyber talent is becoming a costlier investment as the difference in pay for cybersecurity vs. general IT continues to widen
- High-demand low-density positions necessitate an accelerated acquisition cycle with competitive compensation offers that may be unsustainable in the long run
- Professionals everywhere are seeking more flexible work arrangements

Retention Poses Challenges

- Retaining talent can be fragile. Motivators for moving on can include:
  - Burnout, poor work life balance
  - Unclear or unattractive career trajectory, lack of mentorship
- 51% of cybersecurity professionals report stress and risk of burn out, highest recorded phenomena
- Motivators can fuel resignations and represent barriers to future recruitment given the size and closeness of the cyber community

Sources: Bloomberg, CISA, ISC, ISACA, US Bureau of Labor Statistics, CyberVentures, VMWare

Our Approach

Next Peak's Cyber Operational Augmentation proposition helps clients by providing highly experienced talent over a limited period to help clients augment cyber capabilities at a competitive price point.

Next Peak's Cyber Operational Augmentation offering provides access to:

- A network of cyber talent with decades of experience building and running operations in military, government, multinational corporate, and large and small business settings
- Cyber defenders able to both consult and deliver impactful operational activities, integrating client cyber strategies with operations holistically
- Competitive price-point with engagements geared towards operational delivery and co-creation rather than over-the-fence recommendations that can be hard to implement
- Flexible engagements tailored to clients' needs, size and ambitions, rather than out-of-the-box solutions offered by managed service providers (MSPs)
    - Custom projects based on clients' time-line, maturity, requirements

Next Peak Cyber Defenders

Our elite team of Cyber Defenders have:

- Driven global corporate cyber uplifts
- Built & operated advanced cyber ops centers
- Identified advanced persistent threats
- Developed US military cyber tactics manuals
- Established corporate cyber playbooks
- Led response through major cyber breaches
- Deep expertise in MITRE ATT&CK, NIST, ISO, & other cyber defense frameworks
- Built secure remote work systems

COMMERCIAL INNOVATORS

JPMorganChase Bloomberg CROWDSTRIKE

ENDGAME. Morgan Stanley L3

NATIONAL SECURITY LEADERS

CERTIFIED PROFESSIONALS

GSEC GCIH GCFE GCIA aws certified Cloud Practitioner SANS INSTITUTE CISSP

Our team can bring best of breed solutions without the overhead

Use Case #1 – Virtual CISO

Problem statement

You are a small-to-medium company looking to strengthen your cybersecurity posture by developing a cyber program and policies to mitigate cyber risk across the business and operations. However, your company does not have the budget for a full time Chief Information Security Officer (CISO).

Next Peak vCISOs can provide:

- Assistance in designing a cyber program that makes sense for your size, industry, operating footprint, compliance requirement and ambitions
- Support to companies enhance the foundations of cyber programs and ensure operational measures are implemented to mitigate critical business risks
- Trusted advisors to senior leadership on cyber, guiding the planning and implementation of cyber strategic initiatives
- Additional support to serve as a temporary stop-gap as cyber leadership transitions out of roles

Next Peak vCISO Defender Talent

Chirag Arora
CISSP, CCNA, MCP

- Lead developer of the CIS Critical Controls and Control Self-Assessment Tool (CSAT) with the Center for Internet Security (CIS)
- Served in multiple CISO and vCISO roles leading corporate clients through cyber security assessments including FISMA, NIST, and CIS and in developing cyber roadmaps

Alex Beigelman

- Seasoned executive with decades of experience in financial services
- Former CRO of JPMorgan Global Technology & Cyber Risk with oversight of a $10B budget and 50,000 staff
- Former CTO & CISO of UBS Wealth Management Americas
- Former CIO of AEXEO, CITCO's flagship hedge fund platform

Use Case #2- Engineering & Operations

Problem statement

You are a company that is looking to expand your secure service edge security monitoring capabilities, particularly as you move data and operations to the cloud. However, given existing commitments combined with day-to-day responsibilities, you do not have the bandwidth to develop new programs.

Next Peak can provide:

- Security Operations staff augmentation to supplement client security operations, in areas including SOC management, operations, security engineering and monitoring, controls design and implementation, application security and more
- Expertise and assistance in co-designing and co-building new cyber programs that will eventually transition to being managed by in-house teams
- Advisory services to provide expertise on cyber strategy, program and security operations design

Next Peak Security Operations Defender Talent

Alex Cobblah
CISSP, GXPN, OSCE, CNDA, CPT, CEH

- Offensive security and red team expert with 16 years experience in network security
- Deep experience in multiple IT and cybersecurity areas including retail, biotech, cybersecurity, finance and auditing
- Former Senior Offensive Security Engineer at Okta and held multiple red team operator and engineer roles.

Amanda Gorski
CCP

- Over 20 years of cybersecurity experience supporting the Department of Defense and US intelligence agencies
- Cybersecurity Subject Matter Expert for the USSOCOM Command Surgeon's Office
- Supported numerous organizations with expert personnel security and cyber guidance

Use Case #3 – Cyber Risk Governance

NEXT PEAK

Problem statement

Your company has faced negative regulatory feedback around the immaturity of your cyber risk management process, particularly around operational risk management. Third party assessors have also highlighted friction within the organization between cybersecurity operations and risk functions.

Next Peak can provide:

- Hands-on expertise and advice for companies needing to make significant changes to their cybersecurity operational risk management, whether in response to regulatory feedback or desire to strengthen cyber risk mitigation
- An impartial, third-party perspective for companies attempting to re-orient or re-baseline relationships between existing cyber organizations
- Additional capacity to companies in times of significant organizational restructuring and change

Next Peak Cyber Risk Governance Defender Talent

Adam Lange
CEH, GSEC, CISM

- Cybersecurity expert with a wide range of experiences ranging from cyber operations center analysis to policy development
- Built client-facing CTI capability and program for Ernst & Young
- Former member of the US Air Force Computer Emergency Response Team

Shane Ducommun
CISSP, NSTISSC

- Over 25 years of experience in cybersecurity, intelligence and risk management
- Oversaw cybersecurity operational risk management as Executive Director at JPMorgan Chase
- Former US Air Force Officer, serving in the Pentagon, NSA, and several offensive and defensive operations

Use Case #4 – Exercise Programs

Problem statement

Your company recognizes the value of cyber operational and executive level incident response drills and exercises to build muscle memory for effective response in crisis situations. However, your company does not currently have the in-house expertise, capacity or FTE budget to design and run exercises.

Next Peak can provide:

- Exercise Program services to help companies develop or pilot new or expanded cyber drill and exercise programs, certifications or training offices
- Our exercises are crafted to reflect realistic scenarios for participants to respond to, based on individual clients' business priorities, operational structure, network architecture and ambitions
- We work with clients to craft the optimal exercise program cyber operational augmentation engagement on subscription or ad-hoc bases.

Next Peak Exercise Program Defender Talent

Timothy Franz
CISSP, CEH, CSM

- Led major operational exercises for multinational companies and government
- Former Managing Director of US Cyber Command Offensive Operations
- 20+ years experience directing multi-domain red teaming, information security training & multi-disciplined exercises

Jeff Arsenault

- Technical leader experienced in developing advanced network defense frameworks, risk assessment, tactics and training program, virtual range development, and cyber exercises
- USAF Blue Team and NSA Red Team certified operator and team lead, former Cyber Battle Captain at US Cyber Command

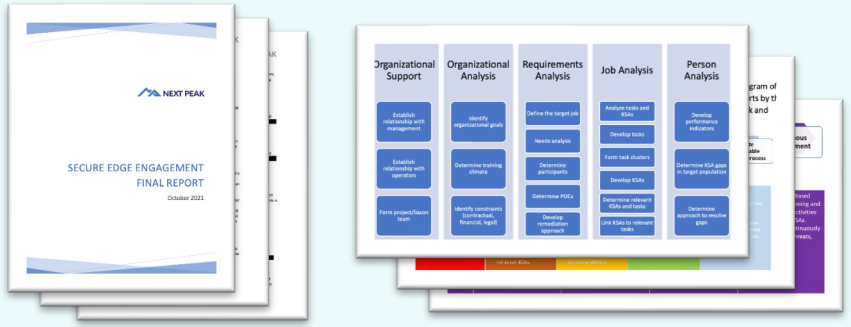
Cybersecurity Knowledge and Experience

Examples of Recent Operational Augmentation Projects

Large Mid-Market US Bank

Secure Edge Staff Augmentation, Training Program Build & Management Uplift

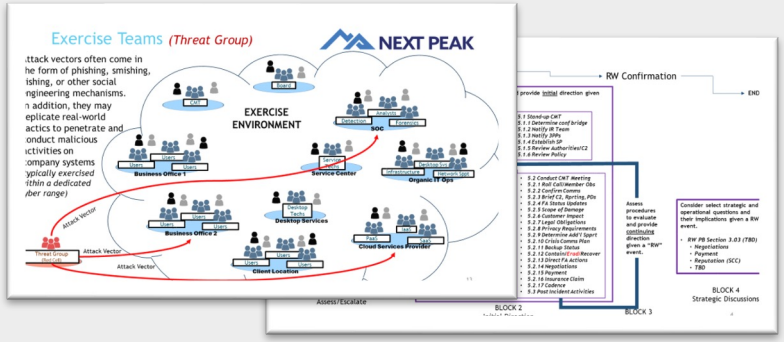
- Provided deep technical experts for staff augmentation to assess and improve company's secure access service edge (SASE) & security monitoring
- Assessed and provided recommendations on governance and sustainment approaches on policies, procedures and standards around critical Secure Edge controls
- Conducted personnel training on key Secure Edge areas including Logical Analysis, SSL Analysis and DNS OSINT
- Developed leave-behind cybersecurity training and certification program
- Assisted in establishing cross-functional governance program across Secure Edge teams reporting up to top executives



US Health Account Provider

Ransomware Playbook Uplift and Tabletop Exercise

- Assessed existing incident response and ransomware playbooks identifying gaps and developing recommendations
- Provided prioritized recommendations of ransomware response playbooks to increase organization business continuity and resilience maturity
- Co-created incident response playbooks alongside client team to ensure unified, repeatable and effective ransomware response
- Engaged cross functional stakeholders to design and execute 2-day ransomware exercise including operational stakeholders and senior leadership testing response capability with newly designed ransomware playbooks
- Conducted after-action briefing, providing a detailed report covering strengths, weaknesses, and recommendations



Our Propositions

NEXT PEAK

Assessments

- Cyber Defense Assessment
- Industry Standards Validation
- Secure Edge Management

Resilience

- Cyber Exercises
- Red Teaming
- Cyber Response Coaching
- Ransomware Preparedness

Advisory

- Virtual CISO Services
- Geo Cyber Risk Services
- Board Advisory & Education

Capacity Building

- Cyber Operational Augmentation
- Security Operations Uplift
- Security Data Discipline
- Post Breach Uplift

Next Peak offers Cyber Workshops for our range of propositions