कार्यबल का विकास

आवश्यकताओं की पहचानना

- अपने काम के बोझ की आवश्यकताओं को पहचानें।
  - अपने संचालन की जटिलता और उस गति का मूल्यांकन करें जिसके साथ कार्यों को निष्पादित करने की आवश्यकता है।
  - बढ़ती क्षमता की जरूरतों पर विचार करें और विचार करें क्या उन्नत तकनीकें हमले के फ़लक को कम करने में मदद कर सकती हैं।
- अपने कार्यबल की आवश्यकताओं को पहचानें।
  - अपने संगठन में साइबर सुरक्षा कार्यबल की योग्यता, लचीलेपन और दक्षता पर विचार करें।
  - आदर्श रिपोर्टिंग संरचनाओं को पहचानें और वहां पर उजागर करें जहां बहु-कार्यक्षमता बेहतर है।
- उनके द्वारा ली गई भूमिकाओं और उनके द्वारा समर्थित व्यवसायिक कार्यों के आधार पर अपने कार्यबल के आवश्यक ज्ञान, कौशल, योग्यता और योग्यता को परिभाषित करें।
- अपने संगठन के मौजूदा साइबर सुरक्षा कार्यबल में महत्वपूर्ण कमी की पहचान करें।
  - भूमिकाओं और जिम्मेदारियों के आंतरिक आकलन के मार्गदर्शन के लिए एनआईसीई फ्रेमवर्क जैसे मौजूदा उपकरणों को लागू करें।

आंतरिक प्रशिक्षण और विकास को आगे बढ़ाना

- कैरियर मैप बनाएं जो आपके साइबर सुरक्षा कार्यबल के लिए उन्नति ट्रैक को प्रदर्शित करता है
- साइबर सुरक्षा भूमिकाओं में प्रतिभावान कर्मचारियों को बनाए रखने और पुन:स्थिति निर्धारण के लिए अपने संगठन के भीतर रास्ते को पहचानें।
  - रूचि और क्षमता के आधार पर साइबर सुरक्षा में गैर-पारंपरिक प्रवेश-बिंदुओं पर विचार करें।
  - अपने संगठन के भीतर अपस्किलिंग और पुनः- प्रशिक्षण कार्यक्रमों का विस्तार करें और पारगमन को प्रोत्साहित करें।
- आंतरिक प्रशिक्षण और स्वतंत्र रूप से सीखने को प्रोत्साहित करें।
  - निरंतर शिक्षा और कौशल प्रमाणन के लिए अवसर खोलें।
- कार्यबल को बनाए रखने के लिए डेटा की निगरानी करें।
  - यह पहचानने के लिए समय-समय पर अवधारित डेटा का मूल्यांकन करें कि क्या प्रशिक्षण और विकास कार्यक्रम कर्मचारी की जरूरतों को पूरा कर रहा है।

बाहरी भर्ती में सुधार

- स्पष्ट, आंतरिक रूप से सुसंगत नौकरी के विवरण लिखकर जॉब पोस्टिंग को मजबूत करें।
  - उपयुक्त कौशल सेट को उजागर करने के लिए एनआइसीई फ्रेमवर्क जैसे मौजूदा उपकरणों का उपयोग करें।
- आवेदन प्रक्रिया के माध्यम से भर्ती पर डेटा इकट्ठा करें, आवेदकों के प्रकार और पिछले कार्य अनुभवों को कैप्चर करें।
  - डेटा एकत्रण को व्यवस्थित करें और साइलो निर्माण को रोकने और टैलेंट उद्गम और विकास का समर्थन करने के लिए पूरी कंपनी में साझा करें।
  - पहुंच में कमी की पहचान करने के लिए समय-समय पर भर्ती डेटा का मूल्यांकन करें।
- उम्मीदवार की क्षमता का आकलन करने के लिए कई संकेतकों पर भरोसा करें।
  - व्यवस्थित हायरिंग के आकलन को लागू करने पर विचार करें।
  - उपयुक्त डिग्री, प्रमाणपत्र और कार्य अनुभव का मूल्यांकन करें।
  - हायर करने का निर्णय लेते समय एक विशिष्ट मीट्रिक (जैसे, इंजीनियरिंग में स्नातकोत्तर स्तर की डिग्री) पर भरोसा करने से बचें।

मूलभूत दृष्टिकोण

साइबर सुरक्षा कार्यबल बनाते समय निम्नलिखित रणनीतिक दृष्टिकोणों पर विचार करें।

1. नई प्रतिभाओं को पैदा करने वाली **आपूर्ति पाइपलाइन** का **विस्तार करें।**
   - क्या आपके विश्वविद्यालयों और तकनीकी कॉलेजों के साथ संबंध हैं?
   - क्या आप साइबर सुरक्षा इंटर्नशिप या अप्रेंटिसशिप प्रदान करते हैं?
2. **टैलेंट ओपनिंग के साथ मौजूदा आपूर्ति की पहचान और मिलान करें।**
   - क्या आपका मानव संसाधन विभाग आवश्यक कौशल को पोस्ट किए गए नौकरी विवरण में कुशलता से दिखला रहा है?
3. **मौजूदा कर्मचारियों** को साइबर कार्यबल का हिस्सा बनने के लिए **पुनः प्रशिक्षित** करें।
   - क्या आपका संगठन संसाधनों को अपने साइबर कार्यबल में स्थानांतरित करके मौजूदा प्रतिभा का लाभ उठा रहा है?
4. **तकनीकी नवाचार** के माध्यम से अपने साइबर कर्मचारियों **की मांगों को कम करें।**
   - क्या महत्वपूर्ण अवधि के दौरान क्षमता वृद्धि करने के लिए आपके तीसरे पक्ष के सेवा प्रदाताओं के साथ समझौते हैं?
5. वर्तमान कार्यबल के बने रहने में सुधार करें।
   - क्या आपका संगठन टीम के प्रतिभाशाली सदस्यों में निवेश कर रहा है?
   - क्या आपका संगठन इच्छुक व्यक्तियों को साइबर सुरक्षा में करियर तलाशने की अनुमति देता है?