

## कार्यबल विकास

### साइबर सुरक्षा कार्यबल विकास के लिए मूलभूत दृष्टिकोण

- आपूर्ति पाइपलाइन का विस्तार करें।
  - क्या आपके संगठन के विश्वविद्यालयों और तकनीकी कॉलेजों के साथ संबंध हैं?
  - क्या आप साइबरसिटी इंटरनशिप और अप्रेंटिसशिप प्रदान करते हैं?
- टैलेंट ओपनिंग के साथ मौजूदा आपूर्ति को पहचानें और मिलान करें।
  - क्या आपका मानव संसाधन विभाग आवश्यक कौशल को पोस्ट किए गए नौकरी विवरण में कुशलता से दिखला रहा है?
- 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?
- तकनीकी नवीनता के माध्यम से अपने साइबर कर्मचारियों की मांग को कम करें।
  - क्या आपकी क्षमता में वृद्धि करने के लिए तीसरे पक्ष के सेवा प्रदाताओं के साथ समझौते हैं?
- वर्तमान कार्यबल को बनाए रखने की शक्ति 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?

### आवश्यकताओं को पहचानना

- अपने कार्यबल 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 आवश्यकताओं पर विचार करें और विचार करें कि क्या उन्नत तकनीकियां हमले की सतह 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 उसे हाइलाइट करें जहां बहु-कार्यक्षमता बेहतर है।
- उनके द्वारा समर्थित व्यावसायिक कार्यों के आधार पर साइबर सुरक्षा कार्यबल के आवश्यक ज्ञान, कौशल, क्षमताओं और योग्यता को परिभाषित करें।
- अपने संगठन के मौजूदा साइबर सुरक्षा कार्यबल में महत्वपूर्ण कमी को पहचानें।
  - भूमिकाओं और जिम्मेदारियों के आंतरिक आकलन के दिशा-निर्देश के लिए एनआईसीई फ्रेमवर्क जैसे मौजूदा उपकरणों को लगाएं।

## 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 के लिए डेटा इकट्ठा करें।
  - डेटा इकट्ठा करने को व्यवस्थित करें और सिलो बनने को रोकने और प्रतिभा उद्गम और विकास का समर्थन करने के लिए कंपनी भर में साझा करें।
  - पहुँच 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 कार्यान्वित करने पर विचार करें।
  - उपयुक्त डिग्री, प्रमाणपत्र और कार्य अनुभव का मूल्यांकन करें।
  - हायरिंग का निर्णय लेते समय एक विशिष्ट मीट्रिक पर निर्भर होने से बचें।

## आंतरिक प्रशिक्षण और विकास को आगे बढ़ाना

- कैरियर मैप बनाएं जो आपके साइबर सुरक्षा कार्यबल के लिए उन्नति ट्रैक को प्रदर्शित करता है।
- स्टाफ को साइबर सुरक्षा की भूमिका में बनाए रखने और पुनः स्थिति निर्धारण करने करने के लिए अपने संगठन के भीतर रास्ते की पहचान करें।
  - रुचि 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 पर डेटा की निगरानी करें।
  - यह पहचानने के लिए समय-समय पर अवधारित डेटा का मूल्यांकन करें कि क्या कार्यक्रम कर्मचारी की जरूरतों को पूरा कर रहे हैं।