Blackstone

Sign In

Search for Jobs

Apply

Alert, Detect, and Response Engineer - Cybersecurity

Apply

Miami

Full time

Posted 30+ Days Ago

20511

Blackstone is the world's largest alternative asset manager. We seek to create positive economic impact and long-term value for our investors, the companies we invest in, and the communities in which we work. We do this by using extraordinary people and flexible capital to help companies solve problems. Our $915 billion in assets under management include investment vehicles focused on private equity, real estate, public debt and equity, infrastructure, life sciences, growth equity, opportunistic, non-investment grade credit, real assets and secondary funds, all on a global basis. Further information is available at www.blackstone.com. Follow @blackstone on LinkedIn, Twitter, and Instagram.

Business Unit Overview:
Blackstone Technology & Innovations (BXTI) is the technology team at the core of each of Blackstone's businesses and new growth initiatives. Serving both internal and external clients, we work to build the next generation of systems that manage risk, create efficiency and improve transparency within the firm and across our broad community of investors and portfolio companies.

BXTI is nimble and entrepreneurial – our open, iterative design processes and rapid pace of development mean that everyone on the team has the opportunity to make an impact from day one. We are problem solvers who can take projects from idea to implementation. We believe in active mentoring and developing excellence. We collaborate to find the best answers for our customers and for Blackstone. We are critical to the firm maintaining its competitive edge.

Job Description:

Alert, Detect, and Response Engineer - Cybersecurity

Apply

As an Engineer, you will also be responsible for implementing new detections and automated responses across the enterprise. He/she will work closely with the red team to identify key areas of risk to the firm in order to design unique, bespoke detections to further enhance the overall security posture.

Responsibilities:

- Supervise and monitor the quality of security operations investigations
- Lead exceptional tier 1-3 operational management, analysis, and investigation of security incidents
- Conduct investigations; correlate and collate the information; and create reports that communicate the results of the analyses to people who need to know them
- Monitor and manage SOC SLA's for compliance
- Represent the Blue Team on Purple Team engagements / efforts to design and build detections
- Work with security engineering team to identify trends in detections and investigations to better inform the engineering process (security by design)
- Core member of the Security Incident Response Team
- Conduct weekly hot-wash meetings to train junior team members on investigation techniques

Qualifications:

- 7+ years in a hands-on technical role in information security
- Experience with cloud native architectures such as AWS, Azure, Office 365 etc.
- Hands on experience with SIEM for detection, security orchestration and automated response (SOAR)
- Working knowledge of a wide range of current network security technologies such as firewalls, proxies, network and host-based intrusion prevention, DLP, vulnerability assessment tools, security information/event management, endpoint security, anti-virus/anti-malware, etc.
- Digital forensics experience such as network analysis, malware analysis, memory analysis etc.
- Development/scripting experience: Python and/or PowerShell.
- Working knowledge of Information Security best practices
- Proven experience with multiple security event detection platforms (and the ability to orchestrate those to a centralized detection platform).
- Ability to self-organize, prioritize activities independently, create documentation and reporting
- Ability to interface with business and technology stakeholders
- Ability to manage stakeholder expectations in the delivery of projects
- Strong written and oral communication skills with the ability to explain technical ideas to non-technical individuals at any level
- B.S. in Computer Science or Engineering or similar technical program
- At least one active security certification: GCIH, GCIA, SPLUNK ECSA, ECIH or other similar certification

The duties and responsibilities described here are not exhaustive and additional assignments, duties, or

Alert, Detect, and Response Engineer - Cybersecurity

Apply

predisposition, veteran or military status, status as a victim of domestic violence, a sex offense or stalking, or any other class or status in accordance with applicable federal, state and local laws. This policy applies to all terms and conditions of employment, including but not limited to hiring, placement, promotion, termination, transfer, leave of absence, compensation, and training. All Blackstone employees, including but not limited to recruiting personnel and hiring managers, are required to abide by this policy.

If you need a reasonable accommodation to complete your application, please contact Human Resources at 212-583-5000 (US), +44 (0)20 7451 4000 (EMEA) or +852 3656 8600 (APAC).

Depending on the position, you may be required to obtain certain securities licenses if you are in a client facing role and/or if you are engaged in the following:

- Attending client meetings where you are discussing Blackstone products and/or and client questions;
- Marketing Blackstone funds to new or existing clients;
- Supervising or training securities licensed employees;
- Structuring or creating Blackstone funds/products; and
- Advising on marketing plans prepared by a sales team or developing and/or contributing information for marketing materials.

Note: The above list is not the exhaustive list of activities requiring securities licenses and there may be roles that require review on a case-by-case basis. Please speak with your Blackstone Recruiting contact with any questions.

To submit your application please complete the form below. Fields marked with a red asterisk * must be completed to be considered for employment (although some can be answered "prefer not to say"). Failure to provide this information may compromise the follow-up of your application. When you have finished click Submit at the bottom of this form.

Similar Jobs (7)

BXTI-Cybersecurity Access Recertification Product Manager, Assistant Vice President

Miami

Full time

Posted 30+ Days Ago

Product Manager - Procuretech - Client & Firmwide Platforms

Alert, Detect, and Response Engineer - Cybersecurity

Apply

BXTI - Enterprise Technology, DevOps Engineer DBA, AVP

Miami

Full time

Posted 30+ Days Ago

View All 7 Jobs

About Us

Blackstone

At Blackstone, we look to attract and retain the brightest minds in the business, hiring professionals across a wide range of disciplines. Our employees are integral to the firm’s identity, contributing to a culture of integrity, professionalism and excellence. It is their dedication and passion for their work that has helped Blackstone become a trusted partner for some of the largest institutional investors in the world.

Read More

Follow Us

workday