## Cyber Threat Intelligence Analyst

5016666 Cyber Security Cyber Risk

Recruiter: Krista Leofanti Email: [kkarger@deloitte.com](mailto:kkarger@deloitte.com)

London, United Kingdom, United Kingdom

Deloitte Global is the engine of the Deloitte network. Our professionals reach across disciplines and borders to develop and lead global initiatives. We deliver strategic programs and services that unite our organization.

### Work you'll do

As a Threat Intelligence Research and Analysis Analyst, you will conduct analysis of and determine relevancy of threats, threat actors’ behavior, understand and evaluate the Deloitte’s cyber threat landscape, and articulate, recommendations for mitigating and detecting threats to senior leaders and technical teams. This position will also aid in producing a comprehensive operating picture and cyber security situational awareness.

The right candidate is a self-starter with excellent research, analytical, technical, and writing skills. This candidate is a fast learner that can comprehend and implement technical concepts as they relate to vulnerabilities, network activity, malware, tools, cyber-attack Tactics, Techniques, and Procedures (TTPs). They can research and pivot on behavioral and atomic indicators, attributing intrusion activity to threat actors; research broad and targeted attacks, and create a variety of reports. The right candidate is curious, tenacious, a problem solver, and rigorous. This is an internal role and will not engage with Deloitte clients.

Responsibilities include:

* Perform technical research into advanced cyber-attacks, malware and other emerging technologies and techniques to identify threats to Deloitte and report on potential cyber-attacks and malicious threat actors
* Perform proactive research to identify, categorize, and produce reports on emerging, new, and existing threats
* Understand and evaluate the cyber threat landscape, and assess what threats are most relevant to Deloitte and the Deloitte executive audience. Analyze threat trends across the network
* Participate in the shaping of new criteria and methodologies to identify, compile, and mitigate threats
* Conduct insightful research on observed and noteworthy threats, as discovered using open and proprietary sources
* Assess behavioral and atomic threat indicators and their fidelity
* Supply actionable recommendations to other teams within the Fusion Center to bolster cyber security efforts
* Coordinate across a global, virtual team to deliver results in an inclusive manner amidst a diverse set of cultures and nationalities
* Responsible for gathering, reviewing, interpreting, evaluating, and integrating information from multiple sources to assess the relevance and significance of developments in your assigned area(s), and preparing complex intelligence products including briefings, summaries, reports, studies, assessments, and estimates.
* Write tactical and strategic assessments under deadlines
* Provide additional support and insight to other teams within the Fusion Center as requested, assisting with incident investigation as needed
* Partake in learning opportunities via new tools and trainings to develop technical and analytical expertise

### The team

The Deloitte Global Cybersecurity function is responsible for enhancing data protection, standardizing and securing critical infrastructure, and gaining cyber visibility through security operations centers. The Cybersecurity organization delivers a comprehensive set of security services to Deloitte’s global network of firms around the globe.

### Qualifications

* Minimum of 1-2 years of experience in information security or intelligence in a cyber threat intelligence or SOC environment
* Excellent English communication skills, both written and verbal
* Strong interpersonal skills and ability to work well with people of diverse cultures and backgrounds
* Knowledge of fundamental threat intelligence concepts
* Knowledge researching and analyzing threat actors, and assessing the level of threat they pose
* Experience and understanding of threat TTPs, malware, most prominent cyberattack methods and tools. Understanding of common malware techniques
* Knowledge of models that describe cyber-attacks (e.g., Cyber Kill Chain, Diamond Model, MITRE ATT&CK)
* Familiarity manipulating data to reveal new insights
* Understanding of the cybercrime ecosystem - topics such as bulletproof hosting, ransomware, criminal affiliate programs, botnets, underground forums and marketplaces, criminal proxy and VPN services, spam, money/reshipping mules, carding, DDoS services, and/or malware development and distribution techniques
* Ability to evaluate cybersecurity vulnerabilities and associated exploits in technologies
* Experience producing and presenting clearly written operational, tactical, and strategic intelligence and writing concise research reports
* Ability to quickly learn and develop proficiency in technical and analytical tools to perform intrusion, link, and pattern analysis
* Experience with open-source investigations techniques and ability to use open-source tools such as VirusTotal, Hybrid Analysis, Domain Tools, etc. to assess indicators
* Ability to communicate recommended defensive actions
* Experience working independently and geographically separate from some team members
* Desire and ability to work in a dynamic, fast-paced environment
* Ability to recognize and deal appropriately with confidential and sensitive information

Required Education

Bachelor’s degree: a cybersecurity-related field, technology-related field, intelligence-related field, or equivalent education-related experience.

Desired Experience and Skills

* Cybersecurity certifications: CRTIA, GCTI, GCIH, CEH, or other related certifications or equivalent
* Communicate with stakeholders with varying levels of technical proficiency
* Experience with MITRE ATT&CK framework
* Foreign language fluency is a plus, especially Russian and Mandarin.
* Experience with formal aspects of threat intelligence (e.g., biases, ACH, etc.)
* Experience and knowledge researching and contextualizing cyber security and geopolitical landscape situations
* Understanding of host and network forensic artifacts and IOCs, identifying the meaning behind them and uncovering malicious activity
* Threat Intelligence Platform software such as ThreatConnect, Anomali, ThreatQuotient, MISP, or other common platforms
* Understanding and/or experience with link analysis
* Ability to use Splunk to perform complex queries and search for relevant cyber event information
* Understanding of networking topics like how basic IP communication works, TOR, proxies, VPNs, other communications obfuscation methods, and how the Internet is organized (technically and administratively)
* Understanding of social media including both formal and informal venues such as forums, IRC, Jabber, Reddit, etc.
* Experience with private sector and other published threat intelligence reporting and its usage towards effective decision-making
* Experience with programming & scripting languages: Python, JavaScript, Java, PHP, and HTML
* Understanding of system/network security and endpoint protection technologies as well as related threat detection technologies (WAF, EDR, IDS/IPS)

### Our culture

At Deloitte Global people are valued and respected for who they are – with opportunities to bring their unique perspectives, talents and passions to business challenges. Our global workspace creates room for individuality and collaboration. Ours is an inclusive, supportive, connected culture.

## Global Security Operations Center Cyber Security Lead Analyst

5014441 Cyber Security Cyber Risk

Recruiter: Krista Leofanti Email: [kkarger@deloitte.com](mailto:kkarger@deloitte.com)

**Same job available in 7 locations**

Deloitte Global is the engine of the Deloitte network. Our professionals reach across disciplines and borders to develop and lead global initiatives. We deliver strategic programs and services that unite our organization.

### Work you'll do

The Deloitte Security Operations team is responsible for detecting and remediating cyber threats across the internal global Deloitte network. We are seeking a Threat Hunt/Lead Cyber Security Analyst to join our world-class Global Security Operations Center (GSOC) and will primarily be responsible to lead the threat hunting initiatives. This new hire lead analyst will also be the main escalation point for sophisticated security incidents.

**What you can do for Deloitte:**

* Identify patterns/outliers within large data sets that match threat actor TTPs, post compromise behavior, and otherwise unusual activity
* Create and modify security SIEM dashboards to clearly identify scope of findings, or monitor activity
* Provide expert analysis, investigative support of large scale and complex security incidents, and in many cases identify incidents for which a technical detection may not be available.
* Perform threat hunting, APT detection, and malware analysis/forensics.
* Conduct dynamic and static malware analysis on samples obtained during incident handling or hunt operations in order to identify Indicators of Compromise (IOCs)
* Lead incidents and mentor other team members
* Help and contribute to build and mature the Standard Operating Procedures (SOPs)

### The team

The Deloitte Global Cybersecurity function is responsible for enhancing data protection, standardizing and securing critical infrastructure, and gaining cyber visibility through security operations centers. The Cybersecurity organization delivers a comprehensive set of security services to Deloitte’s global network of firms around the globe.

### Qualifications

* Hands on experience in conducting malware analysis, DFIR, CTI or Threat Hunting investigations
* Familiarity with offensive/defensive strategies
* 5+ years of work experience in security and event monitoring
* Experience interacting with senior leadership
* Proactive Security Risk Mitigation
* Self-motivated to perform security research using open-source tools
* Communication Skills with Internal customer
* Self-Motivated and task oriented
* Experience with alert triage and advanced log analysis
* A deep understanding of industry frameworks and standards (ie, MITRE ATTA&CK)
* Ability to navigate and work effectively across complex, geographically dispersed teams
* Ability to balance requirements and needs from different customers or stakeholders globally across Deloitte while keeping your eye on the big picture
* Hands on experience in integrating, deploying, and configuring security tools

**(Bonus points if you have)**

* SANS/GIAC - GCIH, GREM, GCED, GCDA

**What Deloitte can do for you**

* Invest in your career growth by providing you with formal and informal development programs
* Empower you to take lead on key projects that may enhance your leadership and team building skills
* Provide you with on-the-job training opportunities
* Give you the opportunity to foster your coaching and mentoring capabilities
* Help you identify and hone your unique strengths
* Connect you with technical & security leads within Deloitte who can become part of your career growth
* Help you embrace leadership opportunities at every step of your career

**Benefits you will receive by working with Deloitte:**

* 100% Remote
* Competitive pay scale
* Empowered well-being
* Paid time off and collective disconnect holidays
* Competitive medical, dental and vision plans
* Paid parental leave
* Physical and mental wellness programs
* Pension plans and 401(k) for retirement

### Our culture

At Deloitte Global people are valued and respected for who they are – with opportunities to bring their unique perspectives, talents and passions to business challenges. Our global workspace creates room for individuality and collaboration. Ours is an inclusive, supportive, connected culture.