CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

RCIA® Certification Program Guide

What is Cyberthreat Intelligence?

Cyberspace has been expanding on a magnificent scale. It's an important alternative to our physical space today, with more individuals and organisations increasingly interacting across mobile devices and multiple online channels. This new era of greater connectivity has led to the explosion of digital data streaming from online portals, cloud space, social and entertainment networks, online transactions so on.

Cyberthreat intelligence ensures reliability of information collected from any source by evaluating its originality and authenticity. Data is first collected under strict supervision, then it is evaluated and implemented Like any other intelligence agency, cyber threat intelligence detects threats and breaches in a system so that an organization or system can deliver services, products or conduct communication appropriately on time.

The Centre for the Protection of National Infrastructure (CPNI), defines threat intelligence as information that can be acted upon to change outcomes.

The process also identifies intelligence gaps. If conditions warrant, cyberthreat analysts suggest or warn others about new requirements and further efforts required to fulfil the information gaps occurring in a system.

Preparing for cyber attacks is a major challenge to organizations today. Responding to sudden, unseen and unwarranted attacks of cyber criminals operating at a global scale calls for qualified and vigilant Cyber Security forces.

Why Cyberthreat Intelligence Analysis?

On the issue of how artificial intelligence (AI) can enhance cybersecurity, Dudu Mimran, chief technology officer (CTO) at Telekom Innovation Laboratories in Israel, suggests two-fold ways: build a global intelligence network for tracking threats across different geographies; and secondly to fund ongoing research to help improve and preserve data privacy.

Juniper Research forecasts cyber-crime to be worth $2.1 trillion by 2019. Gartner's research predicts that spending on cybersecurity will hit $96 billion in 2018, and only increase thereafter. Cybersecurity Ventures says global spending on cybersecurity will exceed $1 trillion cumulatively between 2017 and 2021. Reports from various sectors show that data breaches have been recurrent time and again.

The UK national Cyber Security Centre (NCSC) reported over 1000 cyber attacks in its first year of operation with nearly 600 being classified as significant. And, increase in the rate of cybercrime is expected to bring in its trail, job openings for 3.5 million unfilled cybersecurity positions by 2021. Enter Cyberthreat Intelligence Analysts!

```
var userFeed = new Instafeed({
  get: 'user',
  userId: SitePreferences.INST_USER
  accessToken: S.INST_USER_TOKEN,
  template: '<li class="tiles__tile">
  resolution: 'low_resolution',
  limit: SitePreferences.INST_ENTS,
  after : initInstaCarousel
});
```

The Demand for Cyberthreat Intelligence Analysts

Cyberthreat Intelligence Analysts have been predicted to be the protectors of our assets in the Cyberspace. They know the what, why and how of all security issues. They are the qualified next generation security consultants whom organizations are hiring to detect the nature of security issues impeding their work and how to a ppropriately counter impending threats.

On one hand, the large volume of digital data collected through electronic, human, internal, and external sources of an organization should be sorted, grouped and analysed. On the other hand, the conditions or the circumstances that makes an organization vulnerable to threats also needs a closer look.

What is RCIA?

Upon completion of the program, the student becomes a Rocheston Certified Cyberthreat Intelligence Analyst (RCIA). The program gives the student a detailed overview of the techniques via which cyber intelligence can be gathered, sorted and analysed. Some of the top threats that a RCIA will be made familiar with include:

- Phishing
- Hacking
- Password Cracking
- Keylogging
- Virus or trojans
- Ransomware
- CryptoLocker

Students will also be acquainted with new-age cyber security solutions proposed by giants. For instance, IBM Watson's AI has made a breakthrough in rapid processing of threat data from several incidents of security breach.

Google's new cybersecurity company Chronicle will focus on detecting threats by analyzing and storing data generated by large enterprises. With Google infrastructure support, Chronicle is expected to detect threats faster and at a broader scale than existing systems. Chronicle CEO, Stephen Gillett says, Chronicle will provide "planet-scale" security analytics, combining Google's existing artificial intelligence, machine learning, infrastructure and "near limitless compute" capabilities.

Students also get a peek into how Big Data and Artificial Intelligence help gather cyberthreat intelligence, and the ways in which Machine Learning techniques help capture intelligence.

Benefits of Gathering Threat Intelligence

- Providing information that links the probability and impact of a cyber attack
- Developing a framework for timely analysis and prioritization of potential
- threats and vulnerabilities given an industry's threat landscape
- Applying intelligence techniques to the aggregation and analysis of contextual and situational risks
- Taking corrective actions upon indicators of attack, especially in the
- defense and space technology sectors associated with nations' security
- Developing a strong defense against threat actor's Tactics Techniques and Procedures (TTPs) using advanced threat modeling
- Managing Operational security systems such as Intrusion Detection
- Systems (IDS), Security Information, and Event Management (SIEM) systems do generate threat intelligence inputs based on the industry
- Breaking the cyber-attack lifecycle perpetrated by other nations, that can be via a threat concept known as Advanced Persistent Threat (APT)

Who will Use RICA

Organizations hire cyber threat intelligence analysts to get them to identify potential risks and threats in the digital space. Individuals looking to be engaged as professionals in digital forensics, critical infrastructure will benefit enormously from the program. Across the industries all over the world, the intelligence analyst will be the man or woman of the hour, in the next few years!

Skills You will Learn as a RCIA

Cyberthreat Intelligence analysts assist decision makers in building the right checks and controls that a system requires.

The broad outline of the evaluation they follow to assist organizations take control of their security can be recounted as:

- Strategic intelligence for providing suggestions about the tools that can be useful for defending any threats specific to domain.
- It identifies and assesses malicious domains, and those with low reputation while gathering information from internet.
- Operational intelligence for providing suggestions on how to respond to specific incidents or events.
- Tactical intelligence for providing real-time investigations and day-to-day operational support.

What is the job role of a as a RCIA

A Cyberthreat intelligence analyst has a huge responsibility on hand and requires multifaceted skills:

- Must have a basic knowledge of Linux, Perl, cloud computing, Microsoft Azure, enterprise security, Python
- Be aware of the infrastructure, services, information, applications and users of the organization and must be responsible for researching, investigating and responding to Cyberthreats
- Have experience in threat hunting and technical analysis
- Actively track threat actors and tactics, techniques and procedures (TTPs)
- Manage intelligence collection, security event analysis and new threats detection capabilities
- Conduct intelligence briefings and develop threat summaries
- Consistently share all intelligence inputs, threat ratings, intelligence integration, data standardization and intelligence providers coordination, with the appropriate security management team

- Assist with incident investigation and forensic analysis
- Understand cloud computing and related security issues
- Understand malware analysis, internet security and networking protocols
- Most importantly, must effectively communicate with all levels of an organization, across diverse teams, geographically distributed groups and sectors

Jobs Available to the RCIA

- Senior Risk Consultant
- Forensics Analytics Senior Consultant
- Risk Manager
- Security Analyst
- Counterintelligence Analyst

What is the Pre-requisite for the Program?

You will need to attend Extreme Hacking® NeXTGEN™

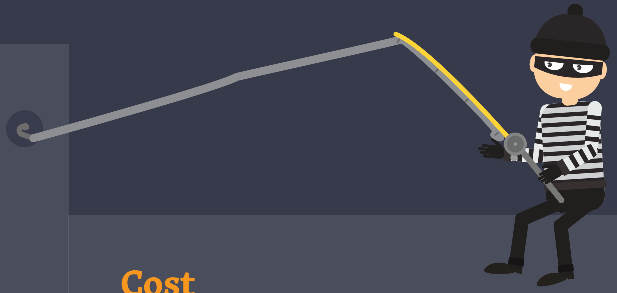
Please visit the RCIA Course outline

https://www.rocheston.com/certification/Cyberthreat-Intelligence-Analyst/

What will be the course structure?

What the course will consist of:

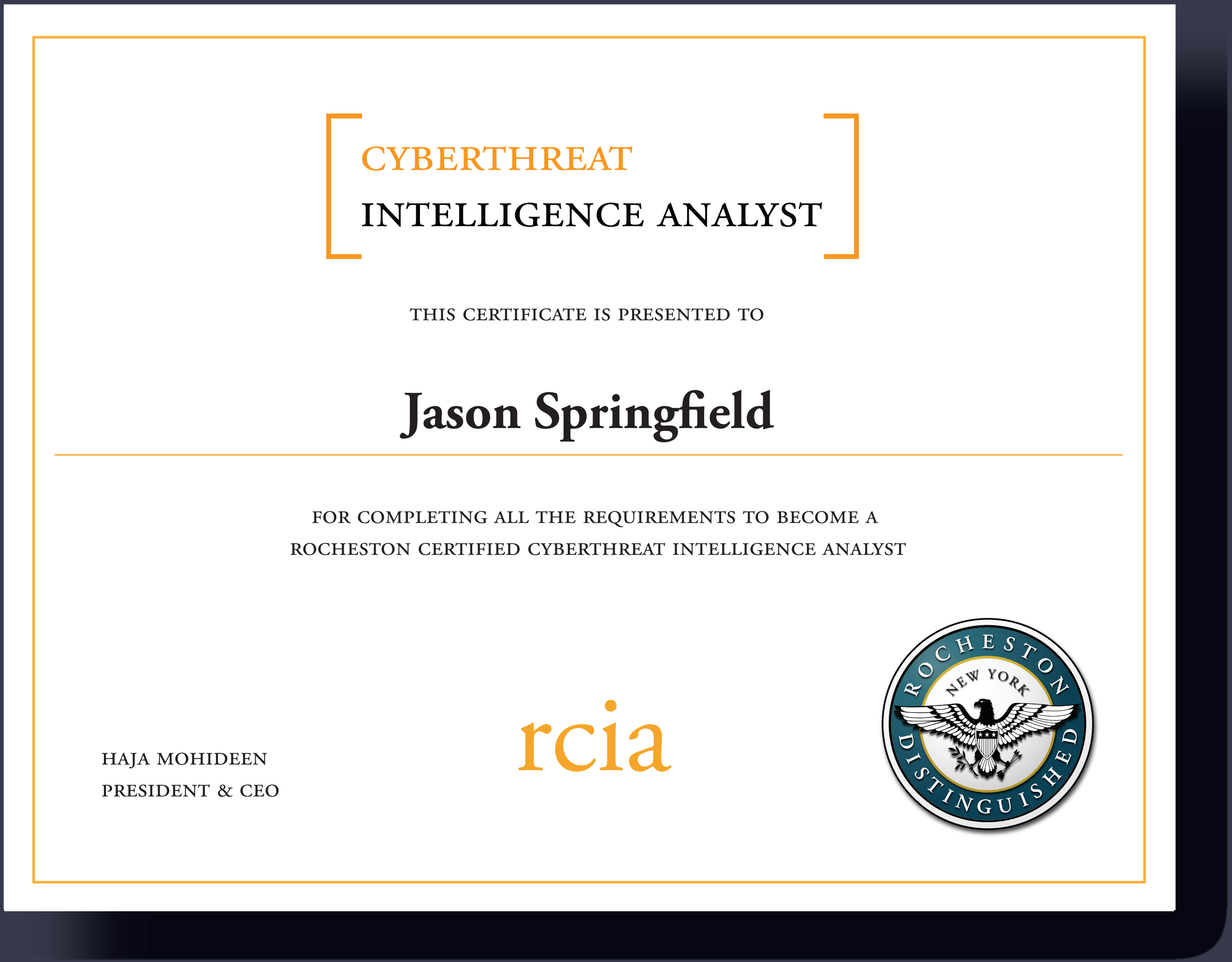
- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The Provision of an Active Web Portal
- Seminars Conducted by Qualified Engineers
- Best in-class environment
- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.



Cost

For pricing in your region, please contact the local distributor.

RCIA Certificate



CYBERTHREAT
INTELLIGENCE ANALYST

THIS CERTIFICATE IS PRESENTED TO

Jason Springfield

FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERTHREAT INTELLIGENCE ANALYST

HAJA MOHIDEEN
PRESIDENT & CEO

rcia

ROCHESTON
NEW YORK
DISTINGUISHED

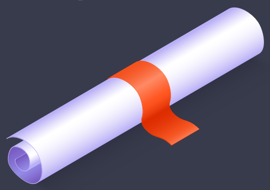
RCIA Exam

The exam will be held on the last day of the program. It will review your understanding of the course and test your understanding by means of specific objective questions.

The access to an online E-learning platform will be given to attendants on registration. It will contain a series of study videos, pre-recorded lectures, white papers, educational animations and power point presentations. The Web Portal can be used to catch-up on a missed session or to view an attended session again.

On completing the course, you will be provided with a RCIA certification. You are free to use the logo as per the Terms & Conditions as a Cyberthreat Intelligence Analyst. You will also receive a welcome kit as a member of the RCIA. Finally, you will be provided with a lapel pin, badge, card, letter of completion and access to the members' portal. The members' portal is an online forum for RCIA to interact. It will be an active portal with weekly updates and news on cybersecurity and cyberthreats.

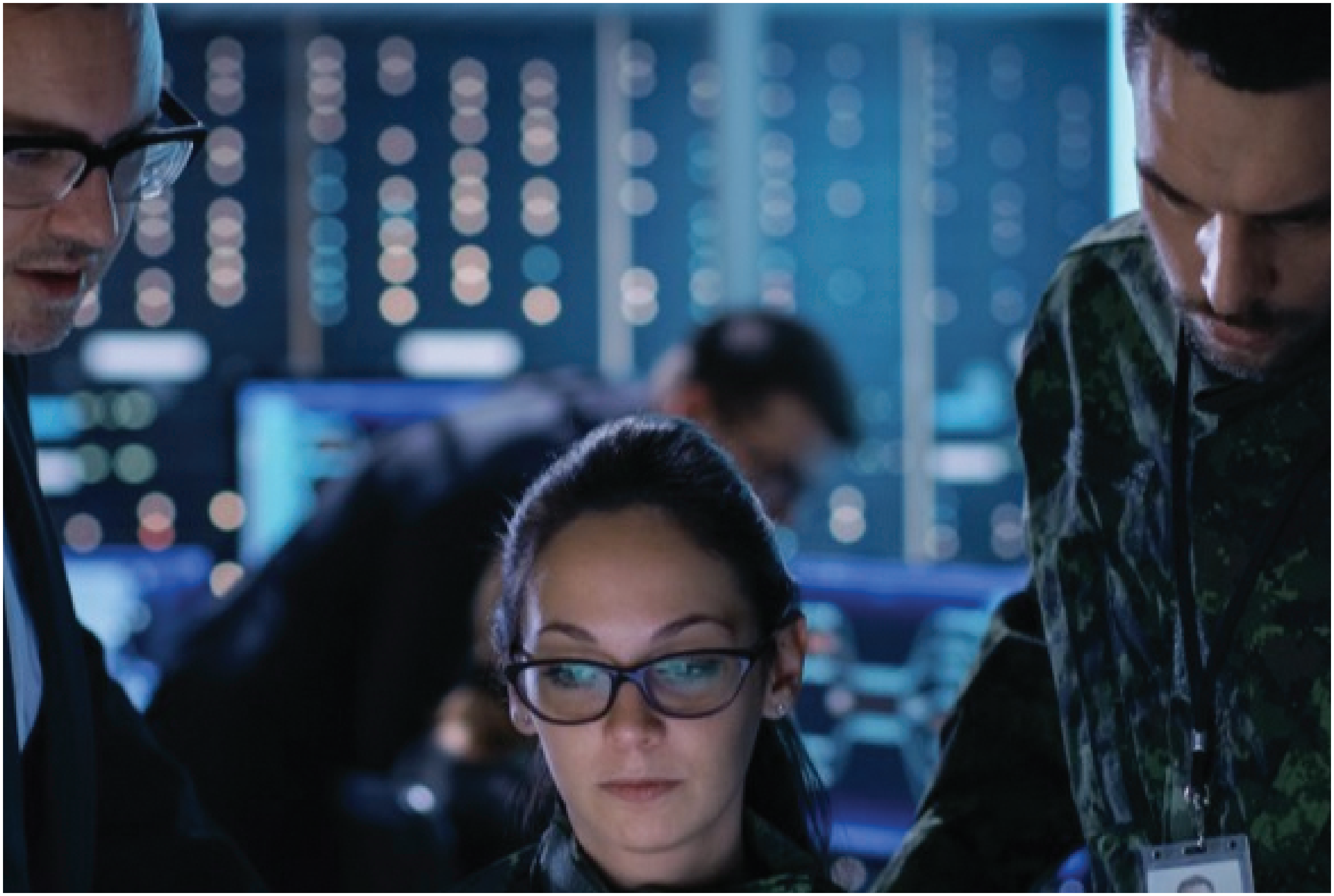
The certification is valid for 2 years. It can be renewed online, with a renewal fee of USD 700 after downloading the updated course material.



CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™



CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL