ROCHESTON®

CYBERTHREAT INTELLIGENCE ANALYST

Certified by Rocheston®

Cyberthreat Intelligence Analyst Certification Program

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. To preserve our precious data in Cyberspace the frontiers of this invisible space should be managed and protected with strong security systems.

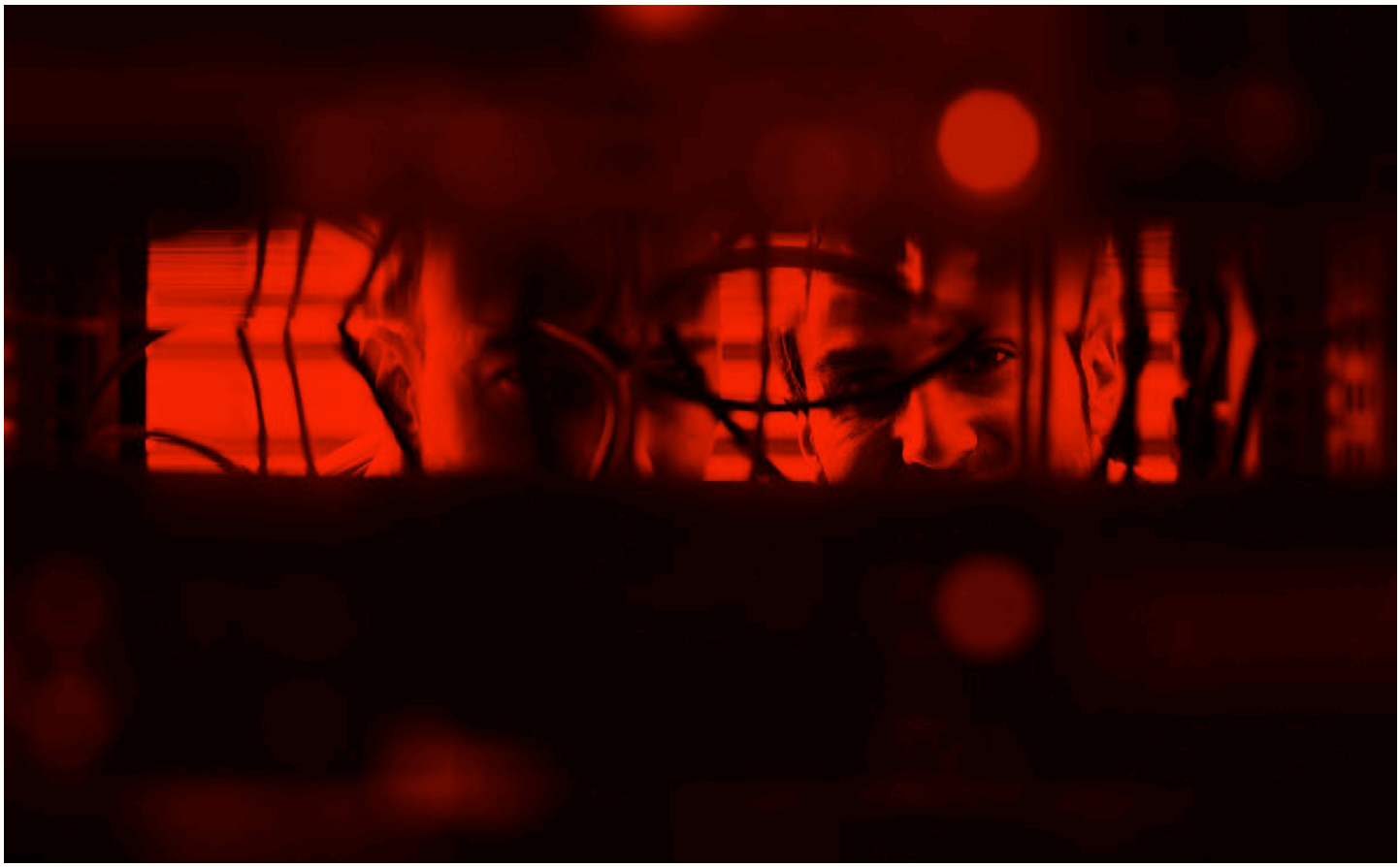
Though routers, network and web application firewalls have been installed to

protect our data assets online, we are increasingly vulnerable to security breaches in our systems. It's not enough to ensure that right security tools are installed in right places, they must work in proper coordination with each other. A breach in the security ecosystem can prove very expensive.

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.

It's time for us to build and maintain strong, resilient Cyber security forces to wage cyber wars against the dark, underworld forces. As foreseen by experts, the future wars will not be fought on land or water but, in cyberspace!

Are you ready to join the world-class Cyberthreat Intelligence Analyst network?



- 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.

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!

Cyberthreat Intelligence Analysts have been predicted to be the protectors of our assets in the Cyberspace. They know 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 appropriately 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 Cyberthreat Intelligence?

Cyberthreat intelligence ensures reliability of information collected from any source by evaluating its originality and authenticity. 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.

Under Cyberthreat Intelligence service, data is first collected under strict supervision, then it is evaluated and implemented. Structured analytical techniques

are implemented to eliminate uncertainties and manage information that can be productive and useful for decision-making – this process converts any incoming information into a valuable piece of intelligence.

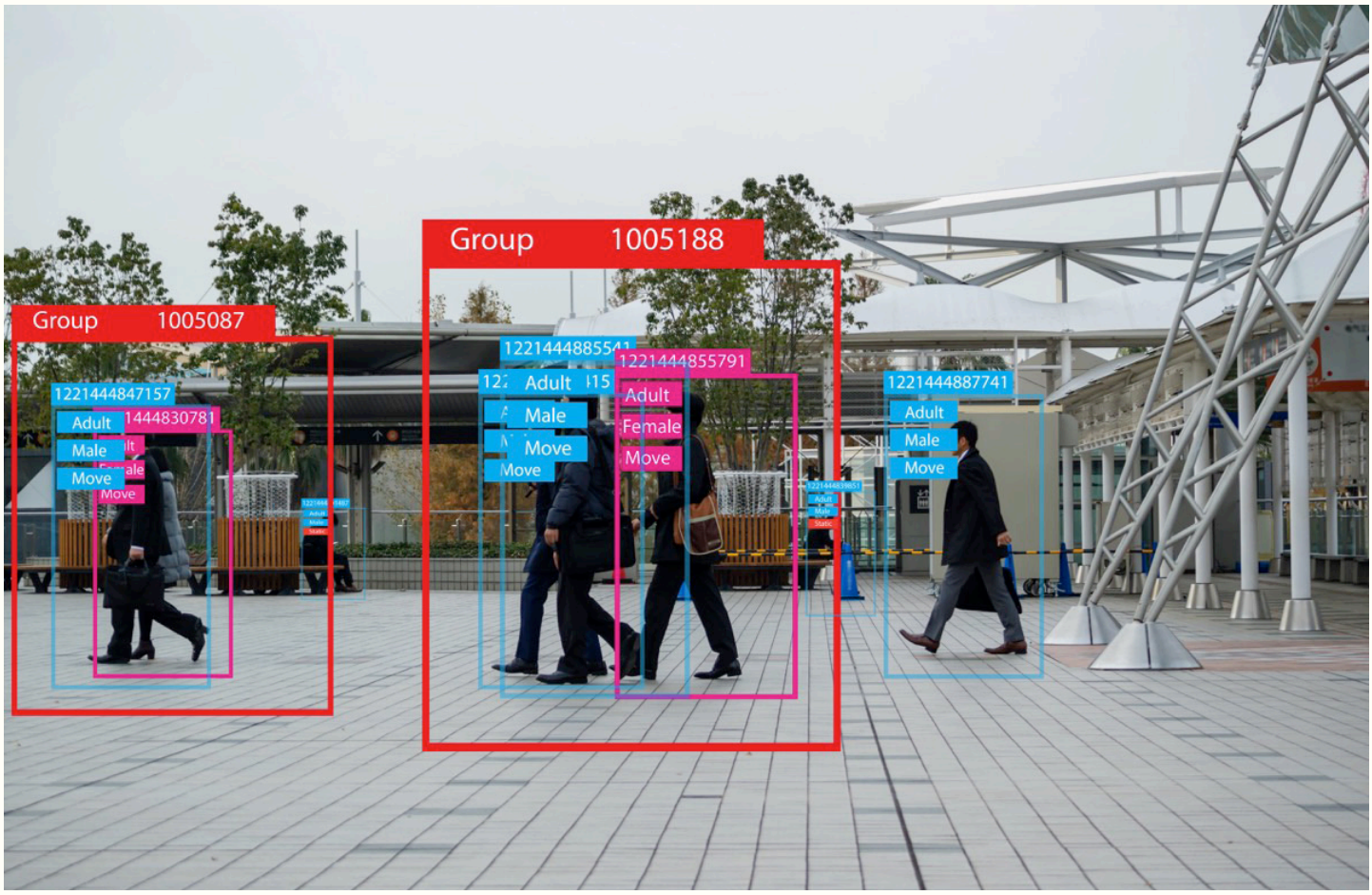
The process also identifies intelligence gaps - detects gaps in information. If conditions warrant, Cyberthreat analysts suggest or warn others about new requirements and further efforts required to fulfill the intelligence gaps occurring in a system.

Which are the Cyberthreats that have increased the demand for Intelligence Analysts?

- Phishing is a cyber attack when individuals impersonate as trusted entities and try to gather information through emails and websites. 93% of phishing emails today have hidden encrypted ransomware.

- Hacking is a cyber attack in the form of an unauthorized system break-in, creeping into an internal network to acquire sensitive data. Hackers use programs that can hide their presence and activities to create havoc with your system.

- Password Cracking is a cyber attack in which encrypted passwords are deciphered with the original alphabets and numeric characters through repeated trails to enter your system stealthily and steal data.
- Keylogger also known as keyboard capturing is used for cyber attack by recording the key sequence or noting strokes on your keyboard. It can target files in your computer and then keyword and smartphone sensors.
- Virus or trojans are used for cyber attacks by installing malicious programs in the hacked system and accessing data.
- Ransomware is a cyber attack that can enter your system to hide files by encrypting them and not releasing them till you paid a ransom. CryptoLocker to WannaCry and NotPetya have caused major crisis for low security websites.



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.
- Latest investigative report from Bloomberg alleges China spied by tucking in a pencil tip-sized spy chip into the computer hardware supplied by an Amazon & Apple components vendor, threatening the US-based businesses.

- Election campaign & voter database hacking is an open secret across the globe that even the super powers US or Russia seem helpless.
- The KRACK attack in 2017 intercepted information exchanged between devices and routers through WiFi, posing serious security and privacy threats.
- In 2017 hackers tried to infect a petrochemical company in Saudi Arabia with malware that could have caused catastrophic explosion if not prevented through.
- In 2017 again, the production at manufacturing plant of Honda Motors were stalled for a day when their network was infected by Wannacry virus, followed by similar attacks on Nissan Motor and Renault. Beazley's research report for 2018 shows WannaCry ransomware attacked 200,000 computers in more than 150 countries.
- Recent study shows financial services and technology sectors experienced 70 percent attacks followed by healthcare and manufacturing sectors facing attacks from cyber criminals. Ransomware, spyware and keyloggers were the widely used malwares.

What is the goal of Cyberthreat Intelligence?

Threat prediction and proactive defense structure development is no longer a choice for companies and countries. In this increasingly digitized world, use of threat intelligence is the priority for mitigating criminal activities.

The objectives and goal of gathering threat intelligence is:

- 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)

How Cyberthreat Analysts can guard organizations against an imminent attack?

Cyberthreat Intelligence analysts assist decision makers in building the right checks and controls that a system requires. Their insights can assist in making budgets and buying equipments. 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. At this juncture, actors, tools, techniques, and procedures are identified; patterns of threats and risks analyzed, in order to keep decision-makers abreast.

Operational intelligence for providing suggestions on how to respond to specific incidents or events. Such suggestions are comparable to forensic report on technical necessities - on how many layered protection from gateway to endpoint does an asset require, what kind of automation mechanism would be ideal under certain conditions and so on.

Tactical intelligence for providing real-time investigations and day-to-day operational support. It updates Cyberthreat intelligence data, arranges awareness programs on general data protection regulations, shows how to integrate them into operations and also implement secured vendor management programs.

What are the new age cyber security solutions proposed by giants of our society?

IBM Watson's AI has made a breakthrough in rapid processing of threat data from several incidents of security breach. capabilities to facilitate the rapid investigation and classification of potential security incidents. IBM QRadar Advisor with Watson is the new AI investigator in which QRadar collects data of potential threats through various sources and then applies cognitive reasoning to analyse and detect a correlation between those data, discover a missing link or identify a pattern in threat information.

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.

Symantec's Endpoint Detection and Response (EDR) and a family of other systems can apply machine learning and behavioral analytics to detect attacks, investigate suspicious activities and quarantine them. Symantec EDR prioritizes for analysing potential attacks.

How does Big Data help you gather Cyberthreat Intelligence?

With network systems getting more complex and the next generation IT networks racing ahead on its fastest set of wheels, sophistication of cyber security threats has grown exponentially. Conventional analytic software, antivirus and SQL-based tooling infrastructure is no match to the latest malware or random Cyberthreat. The number of potentially malicious files that require high priority investigation of its data, exceed a staggering number of 300,000!

Companies need protection from all kinds of data theft and fraud as per the PDR paradigm: Prevent, Detect, Respond. The need of the hour is Threat Intelligence

which is what Rocheston is ready help you with it certification course.

When data itself is in danger Big Data is the one that can come to its rescue!

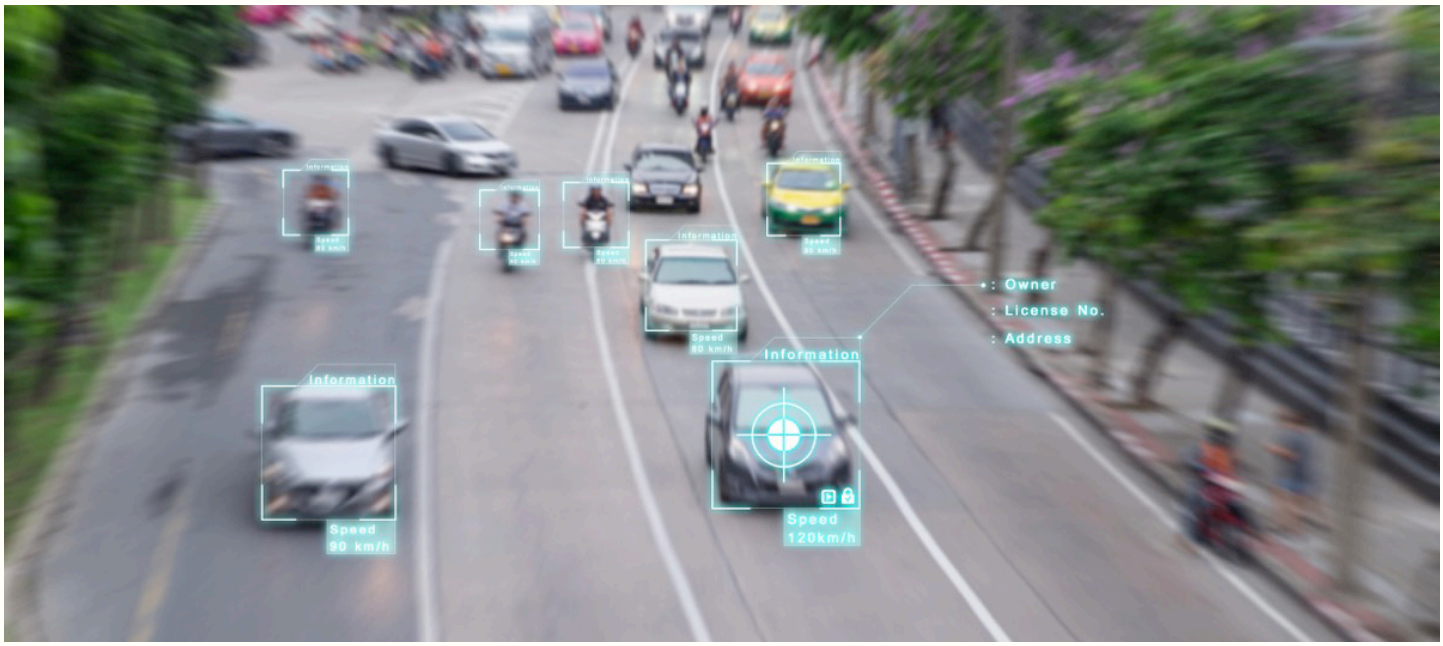
Big Data Analytics has opened the pathway towards gathering Cyberthreat intelligence to safeguard systems security, rendering the traditional solutions obsolete. As per Gartner, 25 % of large global companies have adopted big data analytics for at least one security or fraud detection case. Malware research and analysis based on threat intelligence collected, is becoming more evasive and pervasive. Here is how Big Data Analytics works:

- Threat intelligence analyses the data for macro trends of malware movements to better understand and anticipate the direction of the threat landscape.
- Measure detection performance and analyse statistics on the performance of malware detection to understand which protection technology is providing us the most value.

How AI can enhance Cyberthreat Intelligence?

Artificial intelligence powered cyber security solutions have been predicted to reach $11,047 million by 2025. AI and machine learning (ML) have shown the path to multiply the capabilities of cyber security – detecting malware and network intrusion over large network can be accomplished with higher speed and accuracy. Threat detection is a highly specialized task, enabling machines to learn from past Cyberthreats and gradually adapt to complex data providing better security solutions against advanced threats.

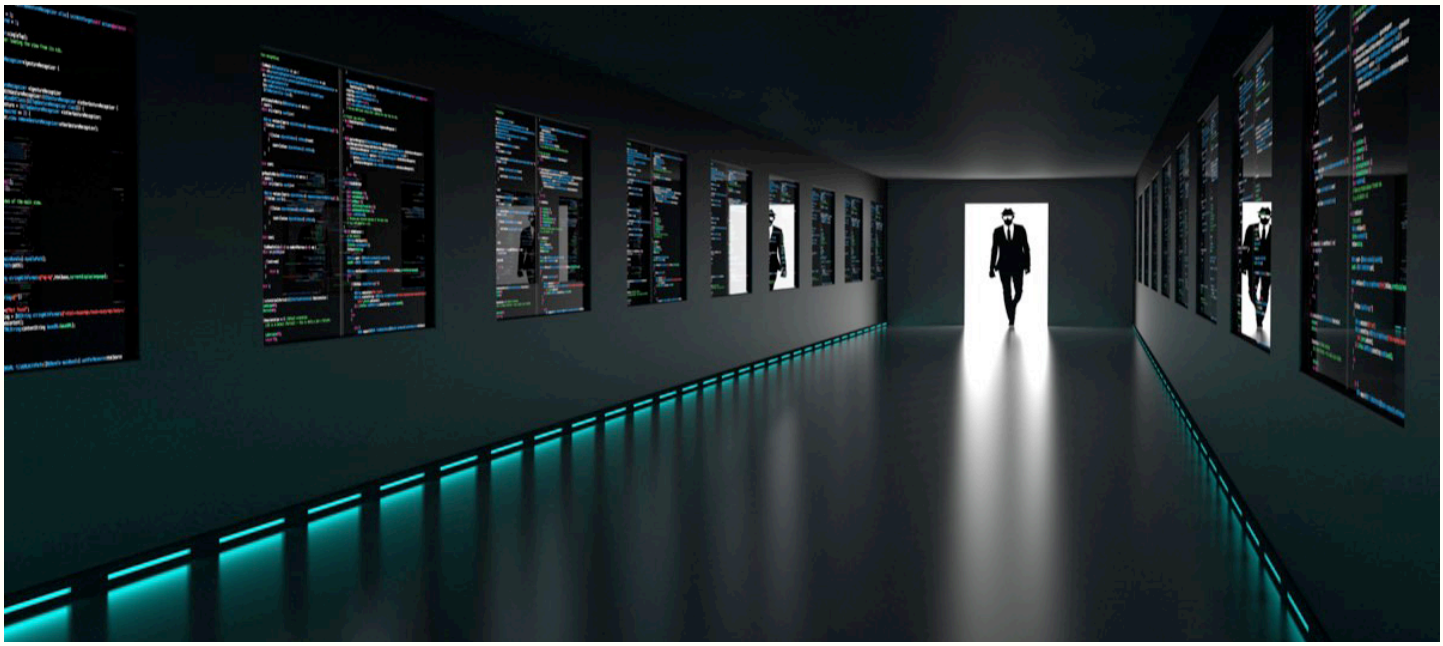
Threat Intelligence Analysts can acquire deeper understanding by analyzing visual representations instead of analyzing rows of data itself. Deep learning, used for studying behavioral analytics are being used to detect anomaly and machine learning algorithms for detecting changes in the baselines of security events in an organization. AI in cyber security promises to bring advanced technological innovations for gathering threat intelligence and effective management cyber-attacks and developing solutions to counter such threats.



Can Machine Learning effectively capture Cyberthreat Intelligence?

Any space or environment, be it an application, social media, mobile, data, cloud computing or Internet of Things (IoT) — all pose a cyber security threat. The very basis of machine learning is to develop a functioning system for extracting information from applying machine learning methods to predict items of substantial threat. This method predicts threat levels using text feature extraction, applying supervised learning models Naive Bayes, Nearest Neighbour, Random Forest and Support Vector Machine such that it can predict un-deployed or emerging attack threats with an 81.77% accuracy.

Machine learning has also become the substratum of Artificial Intelligence, and can extend to data mining process in order to learn patterns, theories, predictions and models from large data sets. The multi-faceted data mining area also includes statistics, artificial intelligence, databases, pattern recognition and data visualization that offers high levels of accuracy and predictions in data analysis.



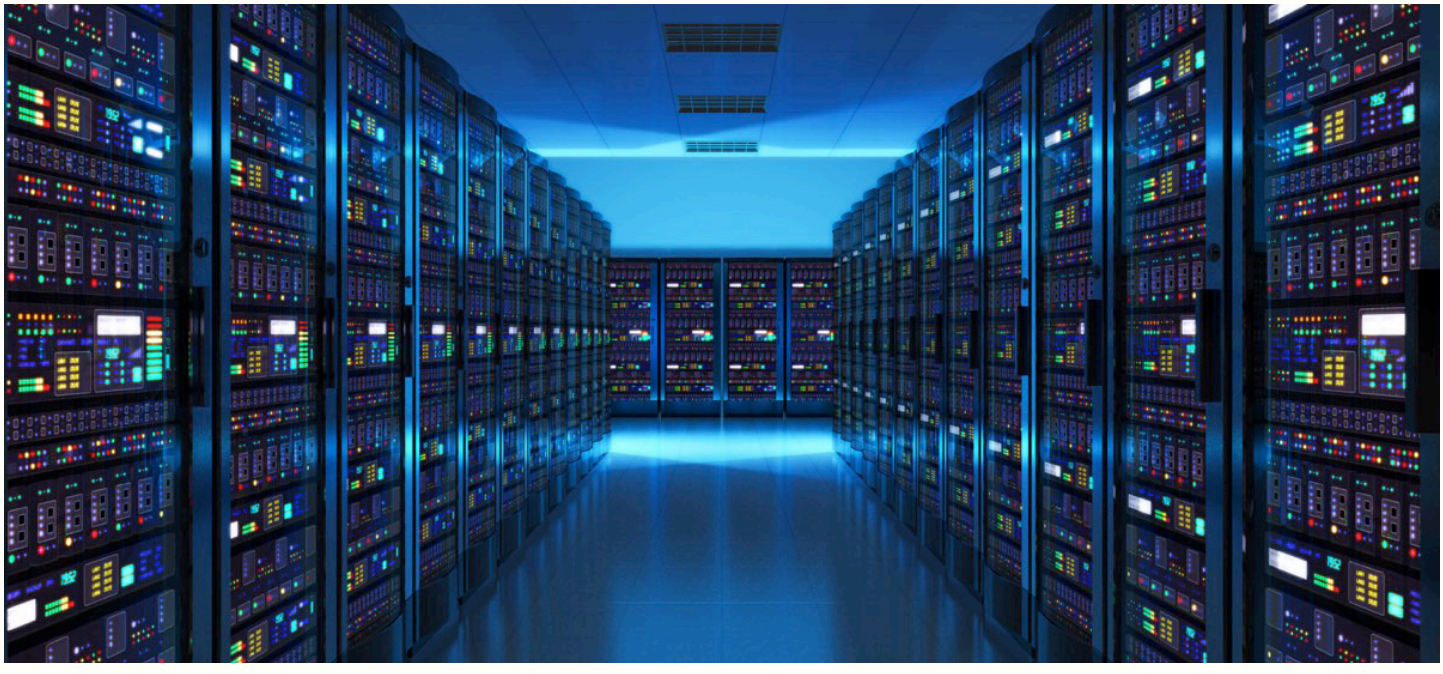
With the kind of Z-level priority attached to threat intelligence gathering, we see that one of Google's latest companies is almost ready to go after a $96 billion cybersecurity industry on a 'planet scale' – the "Chronicle". This platform is expected to solve analytic and workforce problems while delivering global-level security services to large corporations. The organizations also get a forewarning of the probable future attacks through threat intelligence. Different methods like the monitoring of endpoint data to record threat actors in a system.

Artificial intelligence and machine learning enables organizations to gather pre-reconnaissance data that can be used in Cyberthreat intelligence. Pre-reconnaissance data can include anomalies, botnet and phishing detection, as well as the active authentication (Epishkina & Zapechnikov, 2016). The gathering of threat intelligence is the first line of defence in the cyber security infrastructure, followed by the reactive security systems such as intrusion detection systems (IDSs) and mitigation techniques.

How can threat intelligence gathering process be simplified with Intelligent Orchestration?

Intelligent orchestration blends products and processes with human intelligence and machine-based intelligence, to develop a robust system for effective resolution. The inputs and suggestions from experts are captured and codified into IR playbooks, and security technologies provide analysts with the incident context needed to understand the threat and resolve it. The tools used to gather Security information and event management (SIEM) or endpoint detection and response (EDR) tool can be fully automated so that a threat intelligence analyst has more incident context such as obtaining a forensics image or re-imaging machine via a help desk ticket, can be enabled with the click of a button.

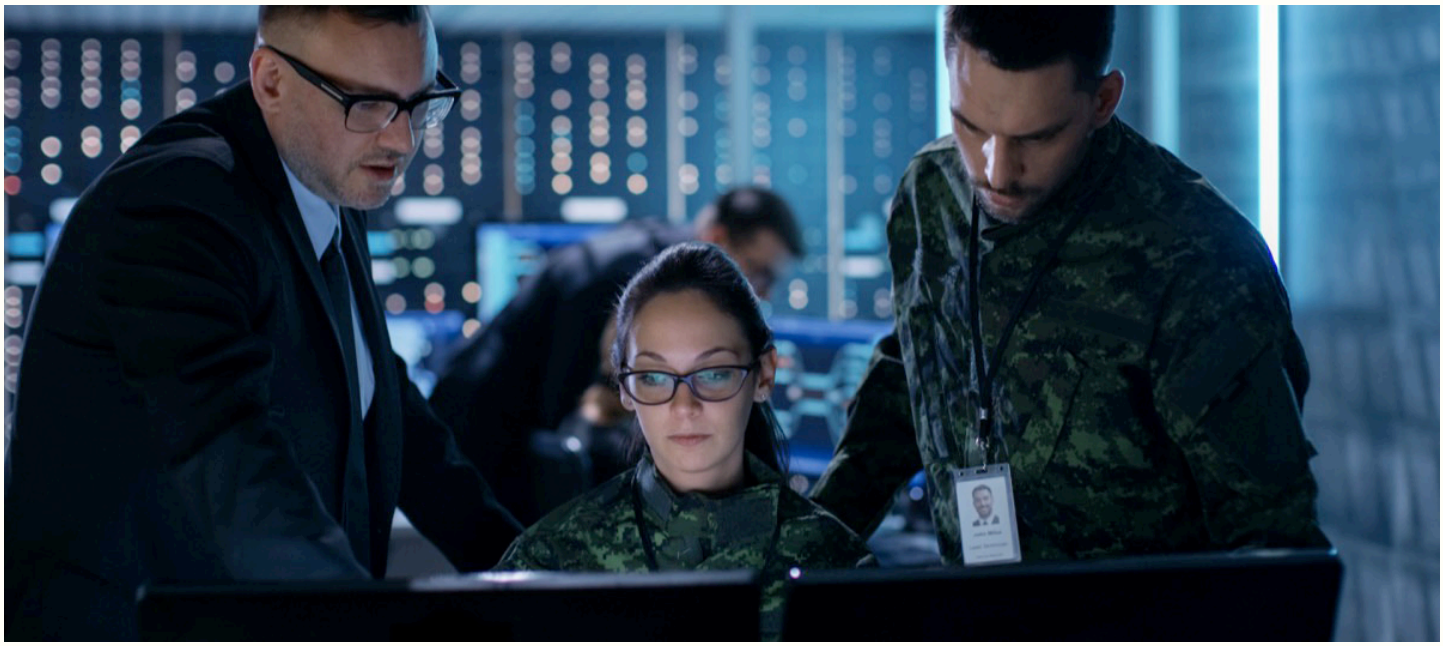
Intelligent Orchestration transfers specific repetitive procedures of work to machines. It gives security analysts time to dabble with special activities of analyzing and developing specific intelligence – to strike fast and on time.



What is the job role of Cyberthreat Intelligence Analyst?

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

What is the Pre-requisite for the Program?

You will need to attend Extreme Hacking® NeXTGEN™

What you will learn?

Please visit the RCIA Course outline

Cost

Course Fee – USD 1299/ -

Exam Fee – USD 799/ -

Exam Retake Fee – USD 400/-

Course Goodies

On Registration, you will be provided with –

1. Course Manuals
2. Exercise Books
3. White papers, resources, and a Rocheston USB
4. Rocheston Bag
5. Rocheston T-shirt
6. Pens, Notepad, etc.
7. Cyberclass® access
8. Cybernetwork® access to online labs

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 Cyberclass® Web Portal

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.

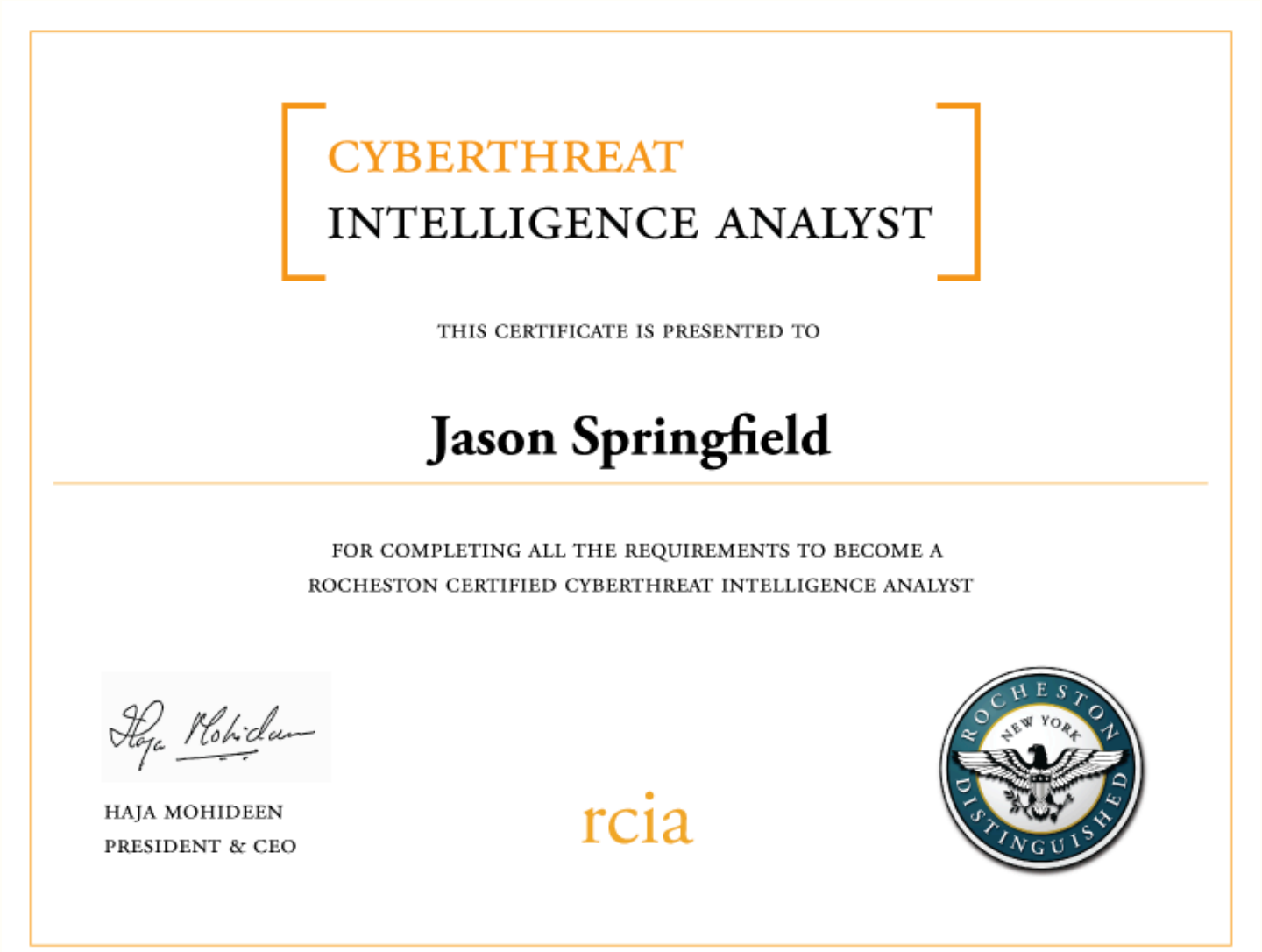
Post Course Completions

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.

Post Course Completions



CYBERTHREAT
INTELLIGENCE ANALYST

THIS CERTIFICATE IS PRESENTED TO

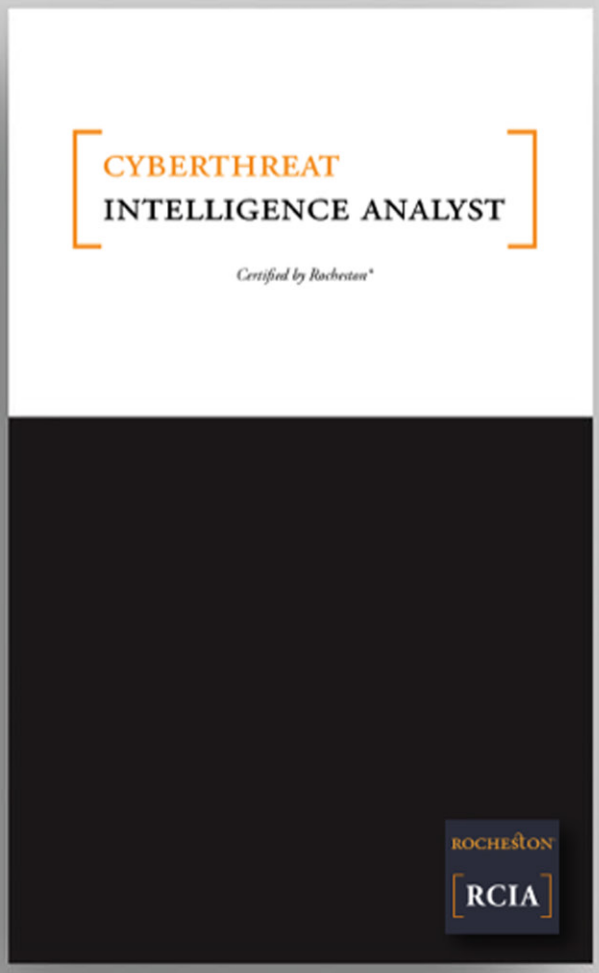
Jason Springfield

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

HAJA MOHIDEEN
PRESIDENT & CEO

rcia

ROCHESTON NEW YORK DISTINGUISHED



ROCHESTON
NEW YORK
DISTINGUISHED