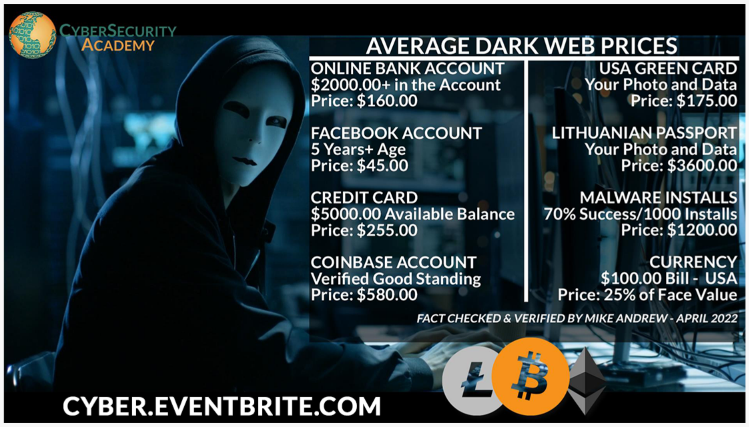
EINPRESSWIRE

CyberSecurity Academy Announces Class on Exploiting Dark Web Intelligence

Training on exploiting dark web intelligence will help organizations of all sizes to bolster security.



CyberSecurity Academy

AVERAGE DARK WEB PRICES

ONLINE BANK ACCOUNT
$2000.00+ in the Account
Price: $160.00

FACEBOOK ACCOUNT
5 Years+ Age
Price: $45.00

CREDIT CARD
$5000.00 Available Balance
Price: $255.00

COINBASE ACCOUNT
Verified Good Standing
Price: $580.00

USA GREEN CARD
Your Photo and Data
Price: $175.00

LITHUANIAN PASSPORT
Your Photo and Data
Price: $3600.00

MALWARE INSTALLS
70% Success/1000 Installs
Price: $1200.00

CURRENCY
$100.00 Bill - USA
Price: 25% of Face Value

FACT CHECKED & VERIFIED BY MIKE ANDREW - APRIL 2022

CYBER.EVENTBRITE.COM

CyberSecurity Academy

SEATTLE, WASHINGTON, UNITED STATES, June 13, 2022 /EINPresswire.com/ -- CyberSecurity Academy, a best-in-class provider of custom digital forensics and cybersecurity services, announced today that they will be providing their live, online, Exploiting Dark Web Intelligence training class this month and that 10 paid scholarships for Ukrainian attendees will be provided. Steve Hailey, President/CEO of CyberSecurity Academy, confirmed today that he is working with leaders of the Ukrainian cybersecurity community to vet the attendees.   For additional information about the upcoming class, see https://cyber.eventbrite.com.

“In addition to the cyberattacks and destructive data-wiping malware infections, we are seeing many more misinformation and disinformation campaigns targeting Ukraine than we did prior to the Russia-Ukraine conflict,” said Hailey. “Chatter and activity on the surface and dark web, IRC, Telegram, and intelligence gathered from threat actors and groups via covert communication channels confirm it. There are countless numbers of people helping Ukraine in a multitude of ways, we are all doing what we can. The upcoming training will assist in an ongoing effort to disrupt the spread of misinformation and disinformation that has been targeting the Ukrainian government and military.”

The terms threat actor, bad actor, and malicious actor are terms used to describe a person or group that is wholly or partially responsible for an action that adversely impacts or has the potential to adversely impact an organization’s assets or cybersecurity. Computer users both at work and at home can become threat actors when they unwittingly fall victim to phishing attacks and other types of fraud. For example, cybercriminals that gain access to computers through phishing attacks can then use the compromised systems as conduits into an organization or to perhaps launch attacks against other entities.

> “Businesses, government, and academia are all vulnerable to cybercrime threats - no one is exempt. Along with traditional intelligence sources, we should all be exploiting what the dark web offers.”
>
> *Steve Hailey - President/CEO*
> *CyberSecurity Academy*

“Ukrainian cybersecurity experts and volunteers worldwide are doing a fantastic job both offensively and defensively in support of Ukrainian cyber operations,” said Michael Andrew, Vice President of Training and Analysis Services for CyberSecurity Academy. “When we (CyberSecurity Academy) heard that General Paul Nakasone confirmed the United States Cyber Command was assisting Ukraine with cyber operations, we wanted to do even that much more to help.”

CyberSecurity Academy emphasizes that intelligence is the most powerful weapon that organizations have against the ever-growing number of cybercriminals and threat actors. Having the right intelligence enables smarter and faster decision-making and provides decision-makers with the ability to cut through the sea of misinformation, hyperbole, and rhetoric.

“Cybercrime is now an industry supported by organized crime and nation-states that are subsidized by the victims of ransomware,” said Cory Quinn of Quinntech Investigations. Ransomware-as-a-Service (RaaS) is now commonplace and enables unsophisticated cybercriminals and threat actors to cause enormous damage. The expertise now needed to profit from cybercrime is not much more than being able to point and click. Valuable information can be gleaned from the dark web if you know where to go. Knowing how to safely gather actionable intelligence from the dark web and the other sources covered in the Exploiting Dark Web Intelligence class is all part of being proactive with cybersecurity.”

ABOUT CYBERSECURITY ACADEMY - www.cybersecurityacademy.com
Since 1997, CyberSecurity Academy professionals have been providing digital forensics, cybersecurity consulting services, and training to a variety of clients worldwide. Company owners Steve Hailey and Mike Andrew are internationally recognized digital forensics and cybersecurity professionals and were the first to provide training in digital forensics for judges of the Federal Supreme Court of the United Arab Emirates, an equivalent of the US Supreme Court. Hailey and Andrew have both served as cyberterrorism experts for DHS and FEMA-sponsored programs and have trained DoD personnel to protect some of the most aggressively targeted information systems in the world. They both developed and currently serve as instructors for the Cyber Defense and Digital Forensics programs at Edmonds College in Washington state, often providing their students with opportunities to work on real digital forensics cases, conduct security audits, and perform penetration testing for a variety of organizations. Edmonds College students utilized the college’s cleanroom to perform data recovery for families of the Oso landslide, also known as the SR 530 landslide, that occurred in northwest Washington state in 2014. Recognized as a “center of excellence” for cyber defense education by the DHS and NSA,

students from around the globe attend Edmonds College to study toward degrees in cyber defense and digital forensics. For more information on Edmonds College, please see www.edmonds.edu.

ABOUT QUINNTECH INVESTIGATIONS - www.quinntechinvestigations.com
Quinntech Investigations has been providing investigative and security services to organizations, government officials, and other VIPs across the globe since 1996. The owner and Senior Investigator, Cory Quinn, has trained with Blackwater (now Academi), secret service agents, and military special forces. The "High Threat Protection Military Movement Team" he served with in Baghdad performed 183 combat missions in 9 months without any loss of life to the team or those they were protecting. The wide variety of services offered by Quinntech Investigations and their team of experts include counterespionage services such as electronic bug sweeps, technical countersurveillance inspections, and TSCM consulting for corporations, government agencies, and the military. www.quinntechinvestigations.com/

Erica Nelson
CyberSecurity Academy
+1 575-200-1323
PR@cybersecurityacademy.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Other