The Internet of Things Security Institute Releases IoT Cyber Certification to address "Smart World" Cyber and Privacy Challenges

SCCISP

FOUNDATION

The Internet of Things Security Institute (IoTSI) announced today that it has released the SCCISP (Smart Cities & Critical Infrastructure Security Professional) Foundation Certification

Gold Coast, Jul 17, 2020 (Issuewire.com**)** - Alan Mihalic, President of the IoT Security Institute describes the SCCISP Certification as an IoT Security Institute educational initiative that provides an IoT security certification and industry-recognized credentialed career pathway for Cyber and Privacy professionals working within or seeking to enter, the IoT-IIoT Smart Cities and Critical Infrastructure sectors.

"Earning the SCCISP illustrates an industry professional has the necessary skills to competently & securely design, implement and manage IoT-IIoT Smart Cities and Critical Infrastructure eco-systems. The SCCISP certification is a response to the increasing need for training specifically developed to address the emerging challenges facing our ever-evolving smart world," stated Mihalic.

The world is Changing. It is Getting Smarter. Smart People, Smart Cities, and Smarter Criminals. The SCCISP prepares next-generation industry professionals with the necessary skills to address the "smart world" cyber and privacy challenges. Cities, Precincts, Buildings, and Critical Infrastructure, are working smart spaces, information portals, and community information exchanges that require appropriate security controls to meet their future potential. In a Smart Cities age, this includes maintaining data confidentiality, privacy, and public safety levels that meet government, community, and corporate expectations. This can only be achieved by providing cyber and privacy industry professionals with the necessary skills and knowledge to address these emerging challenges. The release of the SCCISP Certification provides business, government, and industry a means by which to ensure security professionals have the necessary skills to design, manage and maintain security controls within a built and critical infrastructure environment.

The construction and engineering industries will be significantly disrupted as the IoT transitions from a

new technology into a standard feature of the built environment. While an environment that fully integrates your preferences and activities can offer almost limitless opportunities, this shift can also expose smart eco-systems and all those and "things" associated with them to the increased likelihood of cyber attacks.

Whilst a city, precinct, or building that fully integrates your preferences and activities can offer almost limitless opportunities, this shift can also expose service delivery and critical infrastructure to the increased likelihood of cyber attacks.

Smart Cities & Critical Infrastructure Security Professional:

The rationale for the next generation of Cyber Certification

Cybercriminals are focusing on smart ecosystem design and operational functionality to develop new attack vectors. A collision of building connectivity and smart technology can allow an attacker access to Point of Sale systems via the HVAC network. The convergence of information and operational technology – the software and hardware – has seen the once isolated environment of operational technology connected to the IP network. The cybersecurity industry is establishing a presence within the built environment which reflects these cybersecurity design concerns. The future of smart urban planning will usher in an era of creativity, functionality, and convenience resulting in unprecedented opportunities. Key to this successful building services evolution will be the assurance that private, public, and corporate cyber safety is maintained and protected to community expectations.

Cyber criminals who had previously concentrated exclusively on enterprise networks and online e-services are now targeting industrial control systems (ICS), smart precincts at an increasing rate. The stakes are extremely high They can now target critical infrastructures, such as hospitals, government departments, and power stations. The SCCISP certification is an entirely new approach to implementing and deploying security within these smart environments. It provides a level of expertise that empowers the cyber and privacy professionals working within these industry sectors the skills and methodologies to address these challenges.

Moreover, it provides the training by which to engage with key stakeholders, from an array of industries, to ensure proper security processes and controls are maintained throughout the design and deployment stages. The SCCISP certification is an Industry based approach to cyber and privacy training ensuring employers and industry professionals that SCCISP certified professionals have a broad range of skills, both practical and academic that extend beyond traditional security certification. These skills incorporate the unique security and privacy challenges facing IoT technology service delivery and deployment.

About the Internet of Things Security Institute (IoTSI)
The Internet of Things Security Institute is an academic and industry body dedicated to providing frameworks and supporting educational services to assist in managing security and privacy within an Internet of Things ecosystem.

More information available at iotsecurityinstitute.com