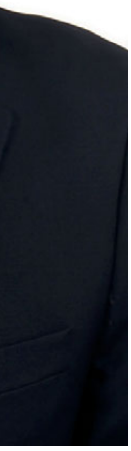
SANS Institute training focus on ICS defence

Industrial systems traditionally prioritise functionality and reliability over cyber security



SANS Institute, which provides cyber security training globally, will hold 'SANS Abu Dhabi 2018' a series of training courses focused on helping regional cyber security professionals enhance their skills in the defence of industrial control systems (ICS).

Historically, ICS systems have been designed primarily with automation and reliability in mind. But given that Shamoon and other internet-based attacks have specifically targeted the industrial sector in the Middle East, there is a clear need to reassess the effectiveness of current ICS defences.

Ned Baltagi, managing director, Middle East & Africa at SANS says, "With this range of training courses, we will equip attendees with the knowledge and skills needed to detect attacks, take necessary steps towards threat containment and remediation, and through the application of digital forensics, understand attacks so as to harden their organisations' defences and prevent reoccurrence."

Professor Thomas Brandstetter, who is teaching the ICS Security Essentials course, observes that both information technology and operational technology roles have converged in today's industrial control system environments, hence the need for a common understanding between the various groups who support or rely on these systems. "Those attending the ICS course will learn the language, the theory, and the basic tools for securing industrial control systems across a wide range of industry sectors."

25%

Of security professionals said they used products from 11 to 20 vendors.

Cisco 2018 Annual Cybersecurity Report

"As IT security risks to businesses grow by the day, cybersecurity is outranking some of the more traditional business risks and concerns."
Bill Conner SonicWall chief executive officer

"The frequency and powerful security threats that organisations are facing are now being recognised and discussed in boardrooms."
Yasser Zeineldin, CEO, eHosting DataFort

Five resilience best practices against attacks by ransomware for financial institutions in the Middle East

Use different credentials for backup storage: The username context that is used to access backup storage should be closely guarded and exclusive for that purpose.

Start using the 3-2-1 Rule: This essentially states to have three different copies of your media on two different media sites, one of which is off site. This will help address any failure scenario without requiring specific technology.

Have offline storage as part of the Availability strategy: One of the best defences against propagation of ransomware encryption to the backup storage is to maintain offline storage.

Leverage different file systems for backup storage: Having different protocols involved can be another way to prepare for a ransomware attack. It's imperative that users add backups on storage that require different authentication.

Achieve complete visibility of your IT infrastructure: One of the biggest fears of ransomware is the possibility that it may propagate to other systems. Gaining visibility into potential activity is a massive value-add.