Arab Security Conference 2021

Event Schedule

Sun, Sep 05, 2021

10:00am

Arab Security Conference 2021 Opening Keynote

10:00am - 11:00am, Sep 5

Opening Keynotes

5th Round of Arab Security Conference 2021 " **Hybrid Edition"**

5th till 7th of September 2021

- Under the Auspices of his Excellency Dr. Amr Talaat
Egypt's Minister of Communications and Information Technology
- Under the Auspices of his Excellency Eng. Mohamed Ahmed Morsy
Egypt's Minister of State for Military Production.

---

5 Subsessions

- **Arab Security Conference 2021 Opening Video**
  10:00am - 10:10am, Sep 5
- **Dr. Bahaa Hasan Opening Keynote**
  10:10am - 10:20am, Sep 5
- **Philippe Wang's Opening Keynote**
  10:20am - 10:30am, Sep 5
- **Eng. Ashraf Serag Opening Keynote**
  10:30am - 10:40am, Sep 5
- **His Excellency Dr. Amr Talaat Opening Keynote**
  10:40am - 10:50am, Sep 5

11:00am

Episodic Image Memory for Solid Digital Identity

11:00am - 12:00pm, Sep 5

Managerial

Secret credentials are indispensable for identity assurance, whereas text-only passwords are hard to manage. Um... Why not consider Non-Text secret credentials?

As an advocate of 'Identity Assurance by Our Own Volition and Memory', I am promoting the concept of Expanded Password System (EPS) that accepts unforgettable images and is deployable on existing text-only password systems, which is intended to be a legitimate successor to the time-honored seals, autographs and text password systems.

The observation that images are easy to remember has been known for many decades; it is not our theme. What we discuss is that 'images of our emotion-colored episodic memory inscribed deep in our brain' is 'Hard to Forget' to the extent that it is 'Panic-Proof.

Speaker

Hitoshi Kokumai Founder and Chief Architect, Mnemonic Identity Solutions Limited

Supply Chain Attacks: What could Possibly Go Wrong?

11:00am - 12:00pm, Sep 5

Managerial

Where do you see your Organization from adopting
Zero Trust Concept?
1- Haven't heard about Zero Trust before
2- Discussion Phase
3- Implementation Phase
4- Already adopting Zero Trust across my Organization

Speaker

Ibrahim Youssef Technical Head - North Africa and Levant at Trend Micro, Trend Micro

12:00pm

Some Stones are Missing- Cybersecurity Holistic Approach

12:00pm - 1:00pm, Sep 5

Managerial

Cybersecurity crime analysis from GRC perspectivec, discussion about the main domain which may impact the organization(s) security environment.
It's time to move to a Risk-Based security strategy.
Risk-based approaches to information security allow organizations to adopt strategies that are tailored to their unique operating environment, threat landscape and business objectives. Risk-based security strategies deliver value to an organization by allowing it to understand the impact of risk mitigation efforts, providing a comprehensive view of risk and filling gaps that may be left by other approaches to security. The use of a risk-based approach fits neatly within the enterprise risk management (ERM) strategies being adopted by many organizations.

Speaker

Bishoy Wasfy Head of Security Governance, Risk and Compliance, CyShield

Threat Hunting 101: Strategy and Yara Rules

12:00pm - 1:00pm, Sep 5

Managerial

A common element in any cybersecurity incident or intrusion gives an intruder access to private information and allows him/her to execute unauthorized/adverse activities such as stealing data, deploying ransomware and more. Join us to understand the magnificent journey of threat hunting, protecting organizations and possibly even finding a new APT.

Speaker

Dr. Amin Hasbini Head of Research Center Middle East, Turkey, and Africa ,Global Research and Analysis Team", Kaspersky

1:00pm

Vendor Risk Management – The arising hidden risk

1:00pm - 2:00pm, Sep 5

Managerial

One of the hot topics that have been arising after the famous SolarWinds incident, vendor risk management became more visual to organizations while they are moving to sustain their security posture. We will discuss the importance of this risk and will tackle different ways to manage this risk across your organization.

Speaker

Wessam Maher Chief Information Security and Risk Officer, The American University in Cairo

Contain the shark attacks: Control the top threats in a telecommunications environment

1:00pm - 2:00pm, Sep 5

Managerial

A highlight towards the top trending threats and security gaps within the telecommunications industry in 2021 and how to remediate and integrate them within the cyber security program.

Speaker

Mohamed Noseir Information Security Manager, Orange Cyberdefense

Security Best Practices on AWS

1:00pm - 3:00pm, Sep 5

Technical Workshops For Beginners

Delve deep into various security aspects of AWS to build and maintain a secured environment. Learn to secure your network, infrastructure, data, and applications in AWS cloud. Use AWS managed security services to automate security Dive deep into various aspects such as the security model, compliance, access management and much more to build and maintain a secured environment. Show security best practices for IAM, VPC, shared security responsibility model, and so on In detail With organizations moving their workloads, applications, and infrastructure to the cloud at an unprecedented pace, security of all these resources has been a paradigm shift for all those who are responsible for security; experts, novices, and apprentices alike

---

Speaker

Magdy Elfaramawy Senior Cyber Security Consultant, EY

2:00pm

Ransomware Attacks and the shifting dynamics of Phishing

2:00pm - 3:00pm, Sep 5

Managerial

The devasting effects of ransomware have continued to grow over the past two decades. We are witnessing ransomware shift from opportunistic attacks to carefully orchestrated attacks. Individuals and business organizations alike have continued to fall prey to ransomware, primarily due to Phishing attacks. Phishing Attacks, on the other hand, have become more sophisticated. The episodes are becoming more severe, the environment hostile, and we are at the receiving end. Is there a cure? If yes, what is it?

Speaker

Akash Agarwal Vice President (IMEA & APAC) at EC-Council, EC-Council

3:00pm

Hacking The DeFi Economy for Fun & Endless Profit!

3:00pm - 4:00pm, Sep 5

Managerial

With the massive rise in the DeFi Economy, billions of dollars are injected into it on daily bases, Unfortunately for Traders, the underlaying Blockchain Technology exposes a lot of financial hacks that allows Trackers (Trade Hackers) to laterally print money!

This session covers the basics of DeFi with deep-drive into Ethereum (Blockchain v2) SmartContracts, Protocols, EVM & Wild Financial Hacks.

Speaker

Mohamed Samy Founder & CEO, Texnomic Ltd

Five Indicators for Situational Awareness

3:00pm - 4:00pm, Sep 5

Managerial

Holistically measuring information situational awareness could help an organization to understand and figure out their major weakness that an adversary could use. We will discuss the five significant measures that could give accurate security situational awareness for the organization, sector, or national level during the presentation.

The presentation will show the linking of Business from high level until reaching the deep technical daily security controls and operations. We will extract the best indicators to give the closest security situation for a system under consideration.

Speaker

Mounir Kamal CYBERSECURITY ADVISOR, Q-CERT

Formal Verification of Smart Contracts

3:00pm - 5:00pm, Sep 5

Technical Workshops For Experts

A smart contract is written in a programming language (commonly Solidity) and then translated into bytecodes. Once a smart contract is reduced to bytecodes, it can be deployed on the blockchain as a contract account at some address. Once deployed no one can change it or apply a patch to it.We should have great confidence that the contract will behave correctly no matter what.
Formal verification is essentially concerned with identifying the correctness of hardware and software design operation. Because verification uses formal mathematical proofs, a suitable mathematical model of the design must be created.

Speaker

MSSASSI Souhail Founder Of ShellBoxes | Penetration Tester | Blockchain Developer, SHELLBOXES

4:00pm

How Digital Maturity affects Financial Institution's performance?

4:00pm - 5:00pm, Sep 5

Managerial

Digital Transformation becomes a buzzword now in today’s business world,
The aim of this paper is to provide insights regarding the digital transformation best practices, and to remove a lot of uncertainty that accompanies the concept. what are the differences between Digital maturity and Digital transformation, the role of effective leadership, the IT dynamic capability, and the cybersecurity effect on the digital maturity of the private financial institution? transformation, and how both are affecting the performance of the private financial organizations and to propose avenues for future research. The results show that digital maturity enhances the performance of private financial institutions by building dynamic capabilities that enable them to adapt quickly to the fast-changing environment, also shows that adopting the cybersecurity strategy at the earliest stage of the digital transformation is positive affects the digital maturity of the organization, it shows as well that leadership has a direct effect on the digital maturity itself.

Speaker

Mohamed Fathy Chief Information Officer, EFG-Hermes SAE

5:00pm

A CISO First 90 Days

5:00pm - 6:00pm, Sep 5

Managerial

In your first three months as a new Chief Information Security Officer (CISO), you will often be tasked with building a security program. For some of us this is the most exciting and stressful part of the job, but this is definitely a very excellent opportunity to start fresh and make a big impact on the security of an organization. We will discuss the very important initial steps that a CISO needs to take in his first 90 days in order to achieve success.

Speaker

Abdulrahman Al-Nimari Cyber Seccurity Director, Self Employed

Cyberattacks on the rise: What to do before and after a cyberattack or data breach

5:00pm - 6:00pm, Sep 5

Managerial

Securing critical infrastructure is vital to ensuring the Arab people have access to services like drinking water, electricity, and food. It is also crucial to protecting high-value industries from cyberattacks, such as the chemical, communications, emergency services, healthcare, information technology, and transportation sectors.

If hackers could breach the critical infrastructure of the sectors listed above, the result could have devastating consequences for organizations. It could also pose a serious threat to global economies and communities. Therefore, successfully protecting critical infrastructures requires government agencies to establish strong partnerships with commercial parties and use appropriate solutions to implement and manage the initiatives.

Protecting critical infrastructure is also reliant on recognizing the risks that could threaten their integrity. This includes attack vectors and network security, as well as issues like equipment failing, the risk of human error, and natural disasters such as weather activity. These risks must be factored into any decision around solutions that enable organizations to detect and identify security attacks and network behavior anomalies.

Speaker

Mohamed AbdelFattah Senior Security Architect, Fortinet

Adopting Zero Trust in a Hybrid Cloud Architecture

5:00pm - 7:00pm, Sep 5

Technical Workshops For Beginners

The session would discuss the meaning of zero trust and how it changes the way we protect systems nowadays. In addition to highlighting a number of attacks that can be eliminated by having zero trusts in place. Finally, we would discuss how to adopt zero trust model between cloud and on-prem infrastructure

---

Speaker

Ahmed Abdallah Security Researcher, Nile University

6:00pm

Real Time Cyber Threats: Daily Hacking Activity Across The Internet

6:00pm - 7:00pm, Sep 5

Managerial

This presentation will analyze and explore the millions of cyber attacks and hack attempts that occur daily across the worldwide Internet, including attacks targeted at specific victims as well as mass non-targeted, opportunistic attacks that must be dealt with by every organization with an online presence.

Who are these large-scale hackers, what are their goals, and how can you best protect your organization from the crossfire of day-to-day cyber threats?

This presentation will include exclusive inside data from AbuseIPDB.com, which uses hundreds of thousands of real-time reports of hacking activity per day to build a map of worldwide hacking attempts (https://www.abuseipdb.com/statistics)

Speaker

Jonathan Weber AbuseIPDB.com

Safety and Security of Interactions between Applications

6:00pm - 7:00pm, Sep 5

Managerial

Emergent software ecosystems, boomed by the advent of smartphones and the Internet of Things (IoT) platforms, are perpetually sophisticated, deployed into highly dynamic environments, and facilitating interactions across heterogeneous domains. Accordingly, assessing the security of these interactions thereof is a pressing need, yet requires high levels of scalability and reliability to handle the dynamism involved in such volatile ecosystems. In this talk, I will present two approaches for detecting unsafe interactions between applications: (1) DINA a hybrid analysis approach for detecting vulnerable interactions between Android applications that leverage dynamic programming features for concealing the interactions; (2) IoTCOM a formal analysis approach for identifying unsafe interactions between smart home applications by considering physical and cyber channels. I will show how the proposed detection mechanisms can efficiently and effectively detect vulnerabilities in contemporary software platforms.

Speaker

Mohannad Alhanahnah Research Assosciate, University of Wisconsin Madison

7:00pm

Cyber Fraud crimes in the age of covid 19

7:00pm - 8:00pm, Sep 5

Managerial

Cybersecurity is considered one of the most important priorities at the present time, as the whole world is connected through the Internet and various information systems, and the development has varied following the emergence of fifth-generation networks and artificial intelligence, which have brought about a great paradigm shift in the use of information technology, and as a result, many types of cyber threats have emerged. And there are many axes of cybersecurity in the comprehensive concept, as it is not limited to securing information systems and preparing tight software, as cybersecurity is represented in a set of axes,

including combating cybercrime and attacks that occur on information systems. Perhaps the most important and most dangerous at all at the present time is cyber fraud that threatens electronic transactions Through the Internet, as the global crises have highlighted the importance of electronic dealings, whether in commercial transactions at the individual or institutional level, or bank transactions, and what they entail in transferring funds, using credit cards, electronic payment and other means of electronic fulfillment, which have become a target for perpetrators and fraudsters for a long time, as they have devised many means To defraud the victims and seize money They and their robbers of their bank card numbers and sensitive personal data, and despite the age of this crime and the multiplicity of its perpetration patterns, as well as the growing capabilities of its perpetrators, cyber threats have emerged in light of the Corona pandemic, in which the whole world has turned to digital transactions at the individual, institutional and private level in a significant increase in cyber fraud crimes. The Spanish police reported a decrease of nearly 50 percent in criminal offenses, while Sweden witnessed a decrease in robberies. Street drug sales decreased, while Austria witnessed a decrease in robbery and theft, with an increase in the percentage of electronic crimes. ”Especially Internet fraud, which has increased dramatically in European countries. The World Health Organization has been affected by a sharp increase in fraud in its name via e-mail to steal Money and sensitive information from users. The British National Crime Agency has detected many people seeking to buy medical supplies online and sending e-mails that defraud users with false medical support while in Germany cybercriminals have exploited people's fears about Covid-19 to send messages. They use malicious content to defraud the victims, ”Interpol issued a warning directed at the organizations that are at the forefront of the global confrontation with the spread of Covid-19 and have also become the target of attacks with ransomware, with the aim of isolating them from their basic systems in an attempt to extort money from them.
This predicts what will happen upon a complete digital transformation. Perhaps the policies pursued by the Gulf Cooperation Council countries aiming at digital transformation will direct us to study the risks and threats that will accompany the digital transformation, which will produce many types of cyber fraud and the consequent damage to the economic cyberinfrastructure, which requires studying and analyzing these risks and threats, understanding their dimensions, exploring their developments, and preparing a cyber strategy that can deal with these risks and threats in a way that deters them, as well as the flexibility to deal with them as a potential threat. In light of the multiplicity of cyber fraud methods between e-mail fraud and cyberbanking fraud in all its traditional and new patterns, we find ourselves facing a threat to trust in commercial and banking transactions in cyberspace, which is the mainstay of transactions in light of the impending digital transformation, so I decided to study and explore these risks, as well as develop a vision for a strategy The countries of the Gulf Cooperation Council can follow to face the potential and expected risks in light of the complete digital transformation in all aspect

---

Speaker

Hossam Nabil Associate Professor

Mon, Sep 06, 2021

10:00am

Enduring from home COVID-19’s impact on business security

10:00am - 11:00am, Sep 6

Managerial

Executive summary: In March 2020, for companies across the world, “business as usual” became business uncharted, as the novel coronavirus spread throughout the nation at an unchecked pace. Faced with shelter-in-place orders in their home counties and states, countless companies transitioned to entirely remote workforces. Predictably, these near-immediate transitions carried with them some setbacks. A remote workforce can become a workforce stretched thin: Communication must adapt to online models of email, chat messaging, and video conferencing; collaboration must move to cloud-based storage platforms; and keeping the business afloat must take into account the unique cybersecurity needs of now-remote workers who are connecting to potentially unsecured home networks while accessing company resources from personal devices—all without the direct support found within the office.
Methodology: I wanted to dig deeper into today’s new, work-from-home (WFH) normal, measuring not just the immediate reaction to the pandemic, but also businesses’ planned cybersecurity strategy for the future.Survey for more than 200 managers, directors, and C-suite executives in IT and cybersecurity roles at

companies across the world. Our survey of roughly one dozen questions tracked respondents' concerns about transitioning to WFH, the impacts suffered due to the pandemic, and their plans to implement long-term security changes moving ahead.

Key takeaways: Our research revealed some concerning trends. We found more devices spread across more locations connecting to more software tools, coupled with an uneven increase in deploying antivirus software. These actions have predictably resulted in serious setbacks for some companies.24% Said they paid unexpected expenses specifically to address a cybersecurity breach or malware attack following shelter-in place orders.20% Said they faced a security breach as a result of a remote worker.18%Admitted that, for their employees, cybersecurity was not a priority, while 5 percent admitted their employees were a security risk and oblivious to security best practices.28%Admitted they're using personal devices for workrelated activities more than their work-issued devices, which could create new opportunities for cyberattacks.survey also found that, despite some of the above setbacks, a majority of respondents scored their organizations rather high when evaluating their readiness to transition to WFH. This may be an example of an often difficult-to-measure phenomenon that we call "security hubris," aka overconfidence in limited security measures deployed At least a quarter of respondents said their organizations froze all or nearly all promotions and pay raises, laid-off employees, or lost clients or contracts. Amongst the worrying trends, however, we found a silver lining. While some of the numbers above may present the picture of an insecure, vulnerable workforce, there is a flipside to the data. The fact is that the transition to WFH has not happened in a vacuum. Stayingcyber secure is not just an exercise in good company governance. Mercilessly, in the midst of all this, threat actors have pounced.

How prepared were companies transitioning to WFH?

COVID-19 caught every company, large or small, off-guard. Organizations' security budgets may have increased year-over-year and their defensive measures may have become more proactive—but few survey participants could admit they were fully prepared for an immediate transition to work-from-home en masse. Less than 16 percent of survey participants gave their organization a perfect score on WFH readiness. Still, a significant percentage of respondents expressed high levels of confidence in how prepared their company was for the move to remote work. To understand the volume of work IT teams would need to tackle in the transition to WFH, we asked survey participants to tell us the percentage of employees that were moved to a WFH model. About one-third of respondents (33.2 percent) moved 81–100 percent—if not all—of their employees home. And 142 respondents, or a little more than 70 percent, moved 61 percent or more of their workforce to a WFH model. For companies with fewer than 700 employees, 42.9 percent moved 61- 80 percent of their workforce home. On the other hand, for companies with 700 employees or more, 37.9 percent moved 81-100 percent of their workforce home Among our respondents from the four major regions of the United States—the Northeast, South, Midwest, and West—organizations from the South moved more employees to WFH (33.2 percent) than any other region. The Northeast trails behind in a distant second (21.3 percent), with the West following closely on its heels at 20.3 percent.33% moved 81–100% of their employees home. 70% moved 61%+ of their workforce to a WFH mode 43% of Companies with 100–700 employees moved 61-80% of their workforce home83% of companies with 700+ employees moved 81-100% of their employees home.

Ranking WFH preparedness To measure participants' confidence in their WFH readiness, we asked managers, directors, and executives across business sizes, US regions, and industries to rate how prepared their organization was to transition to working from home on a scale from 1–10, with 1 representing the least prepared and 10 representing the most. Of the 202 respondents, the average ranking was 7.23. In fact, roughly three-quarters (73.2 percent) of those we surveyed gave their organizations a score of 7 or above on preparedness for the transition to WFH. On the flip side, only 14 percent scored their company a 4 out of 10 or less. Overall, IT leaders were confident that they were prepared to transition to a WFH setup. Among IT leaders surveyed, directors of companies with more than 5,000 employees were the most confident group when rating their company's cybersecurity posture, giving it an average of 8.2 out of 10. In fact, following close behind were directors from organizations with 350–699 employees, with an average of 8.16. However, the pattern stops there, as not all directors felt as confident about their WFH preparedness. In contrast, directors and those in executive/C-suite positions of companies with 700–1,249 employees were the least confident, giving their organizations an average rating of 6.11 and 6.5 out of 10, respectively. Managers belonging to these companies, however, did not share this view. Their ratings bucked the trend hard, with an average of 8 out of 10.

Which WFH challenges were respondents most worried about?

The shift from working in the office to working from home did not erase cybersecurity problems that were already there, pre-COVID. If anything, organizations were presented with new, compounding challenges that had to be addressed without delay.

Companies that were able to successfully transition to WFH did not do so free from problems: More than half of IT leaders surveyed reported facing at least three of the challenges listed in our questionnaire. The challenge cited most by respondents was training employees on how to be security compliant at home (55.4 percent), followed by setting up work or personal devices with necessary software (53.5 percent). Fifty-one percent of participants felt shifting to a new, remote model of communication was a challenge as well. The challenge selected by the fewest respondents was ensuring work/life balance at 36.6 percent.

Organizations' biggest challenges to WFH

55.4% Training employees how to most securely and compliantly work at home
53.5% Setting up work or personal devices with new software to continue current responsibilities/roles
51% Shifting to a new, remote model of communication and/or collaboration amongst employees
47% Serving employee needs through limited IT resources
45.5% Finding the right cybersecurity tools to support employees at home
36.6 Ensuring work/life balance
Employee cybersecurity awareness Despite finding training employees on security compliance to be a challenge, 47 percent of respondents were confident that their employees were “very aware” of the cybersecurity best practices they needed to follow at home. A much smaller portion (17.3 percent) believed their employees were “acutely aware and mindful to avoid risk.” Only 5.4 percent of IT leaders said their employees were “oblivious and risky.”
Employee awareness of cybersecurity best practices when WFH
47% Very aware 18.3%Aware but not a priority 17.3% Acutely aware and mindful to avoid the risk
11.9%Slighly aware5.4% Oblivious and risky
Respondents in director and executive positions expressed more confidence than managers in their employees’ awareness of cybersecurity procedures while working remotely. While 20.5 percent of executives said their staff was “acutely aware,” just 16.2 percent of managers felt the same. Conversely, only 1.7 percent of directors stated their employees were “oblivious and risky” compared to 7.6 percent of managers.
Managers, directors, and executives expressed similar levels of faith in their employees, though directors and executives felt slightly more confident.
Biggest cybersecurity concerns What are your biggest cybersecurity concerns with remote work?
29.2% Difficulty in onboarding remote employees when necessary to prevent unauthorized future access
37.6% Difficulty managing new devices using remote work resources
22.3% Increased risk of ransomware attacks
27.7% Increased malware attacks overall
45%Devices may be more exposed at home, where employees feel safe, but others may have access to their devices and may inadvertently compromise them
37.1% Our IT support may not be as effective in supporting remote workers
31.2% My employees may be using unauthorized and unmanaged “shadow IT” tools to share company and customer data
21.3% My employees lack proper cybersecurity training to act intelligently in order to avoid cyber threats
36.1% My cloud collaboration tools may not provide adequate cybersecurity (concerns of “Zoom-bombing,” for instance)
36.6 % My employees may not have adequate cybersecurity protections for their personal networks and devices
When asked about their biggest cybersecurity concerns now that all or a portion of their employees are working remotely, it is clear that managers, directors, and executives are most concerned about other individuals in the home who have access to an employee’s device and might inadvertently compromise it (45 percent). Other concerns that stood out are difficulties associated with managing devices using remote work resources (37.6 percent), the possibility of IT not being able to support employees efficiently (37.1 percent), and the general lack of adequate cybersecurity measures over resources, including cloud collaboration tools (36.1 percent) and personal networks and devices (36.6 percent).
What actually happened: the bad news
Respondents’ concerns were largely founded in reality. As we learned from our survey, some of the same fears expressed by IT leaders later materialized in the transition to WFH. Our survey found that 23.8 percent of the respondents ran into unexpected expenses specifically to address a cybersecurity breach or malware attack. And nearly 20 percent (19.8 percent) stated they faced a security breach because of a remote worker.
23.8 % of Respondents’ concerns were largely founded in reality. As we learned from our survey, some of the same fears expressed by IT leaders later materialized in the transition to WFH. Our survey found that 23.8 percent of the respondents ran into unexpected expenses specifically to address a cybersecurity breach or malware attack. And nearly 20 percent (19.8 percent) stated they faced a security breach because of a remote worker. 19.8% Faced a security breach as a result of remote worker respondents said they also suffered from cyberattacks and security breaches as a direct result of shelter-in-place.
Let’s briefly put that 19.8 percent statistic into perspective. Remember that all it takes for a company to suffer a security breach as a result of a remote workforce is to compromise just one remote employee. As our survey showed, a remarkable 98 percent of respondents said their organizations have moved at least 21 percent of their employees into remote positions. Further, the remaining 2 percent of respondents said their organizations moved anywhere from 0 to 20 percent of their workforces into remote positions. With these numbers, it’s safe to assume that nearly every company out there today has at least one remote employee, and thus is vulnerable to this type of threat. Further, it is important to point out two significant contributing factors that impact cybersecurity for remote workers. One: Workers that suddenly transitioned to remote work found themselves working from a different environment, outside of the company’s security perimeter. Two: Some of the employees had to work on different, unfamiliar devices. Both of these factors

contribute to a weakened security posture overall. What negative financial impacts has your organization experienced following the shelter-in-place orders?
55% Froze all/nearly all hiring 48% Restricted travel expenses 37.6 Froze all/nearly all promotions, pay raises 30.7% Laid-off employees24.8% Lost clients/contracts
In fact, 31.2 percent of our respondents admitted they sometimes used personal devices for work and a frightening 27.7 percent said they used their personal devices more than the device provided by their workplace. Worse: 8.4 percent never even received a work-issued device for remote usage. Only 39.1 percent adhered to a strict regime of only using work-issued devices for the workload. As we know, though, the effects of WFH and of the coronavirus pandemic extend beyond cybersecurity impacts. Companies have also suffered broad financial losses.

Speaker

Mohamed Sadat ISACA Board Member, ISACA

Attacking & Securing Kubernetes Clusters

10:00am - 12:00pm, Sep 6

Technical Workshops For Experts

This session aims to explain how Kubernetes works and the effective role it plays in the Devops lifecycle. The session also discusses different techniques in which Kubernetes Clusters can be attacked, explaining some real world scenarios for those attacks and the best practices through which to protect them from cyber attacks.

Speaker

Mohammad Khreesha Cybersecurity Manager, Baaz, Inc.

Threat Hunting using Machine Learning

10:00am - 12:00pm, Sep 6

Technical Workshops For Experts

The session is about how we can use machine learning algorithms in threat hunting to predict malicious network traffic from the normal one.

The idea is divided into three phases:-

1- Data Processing: where we take the network traffic whether it's malicious or not from PCAP file or real-time from network sensors, and extract from them all the HTTP headers, and convert these headers to datasets, and divided them into 90% to the training data and 10% to the testing data.

2- Training Phase: where we take the normal and malicious training data and perform the Naïve-Bayes theory on them (we implemented the Naïve-Bayes theory from scratch to absolutely fit our training model and to increase the success rate).
Then we generate a text file that contains all the calculations of the training model (probability of normal HTTP headers, probability of malicious HTTP headers, number of total normal words, number of total malicious words, unique words, probability of normal class, and probability of malicious class), and we will use this file and all these calculations in the testing phase.

3- Testing Phase: where we take the testing data to test it against the training model, and load the training model from the previously mentioned text-file and perform the testing and calculations between these two, where the algorithm predicts to which class this test case belongs, as you can see, we perform the calculations and predictions on the remaining test data that we divided in the first and we don't know the

types of these tests and we don't include them in our training model, so this test data is unknown to us.

The training model can successfully predict all the types of test data whether it is malicious or not without knowing the type of this test data based on the Naïve-Bayes machine learning algorithm and our training model.

And as you go you can continuously include new training data inside our training model to increase its efficacy and increase its success rate.

Tool implemented to do the mentioned theory: https://github.com/hassan0x/Chimera

---

Speaker

Hassan Saad Cyber Security Analyst, Etisalat Misr

11:00am

Network Equipment Security Assurance Scheme

11:00am - 12:00pm, Sep 6

Managerial

This presentation will provide an introduction to GSMA's Network Equipment Security Assurance Scheme (NESAS) and will include the following; • Importance of supply chain security • Need for security assurance • Overview of GSMA and 3GPP defined NESAS programme • Progress made to date on vendor auditing and product evaluations • NESAS benefits • Ensuring successful outcomes

---

Speaker

James Moran Head of Security, GSM Association

12:00pm

SOC From Cyber Deterrence Perspective

12:00pm - 1:00pm, Sep 6

Managerial

Security Operation Centers are usually composed of 3 tiers, usually, the implementation of a SOC starts by getting Tier 1 (SOC Analysts) onboard then Tier 2 (Incident Responders) & finally, and maybe never Tier 3 (Threat Hunters) ... But what if this sequence is drastically reducing the value of the SOC and making the enterprise more prone to lose? What if there was a better sequence of implementation that secures better the enterprise, increases the SOC value and decreases security losses? Enterprises need to be proactive rather than reactive in the way they handle security and must focus on preventing incidents while they remain threats rather than wait for the disaster to happen and handle it as an incident. In this session, we will look at SOC from a proactive rather than reactive perspective, from an attacker rather than attack perspective, ... From a security ... Rather than compliance perspective.

Speaker

Osama M. Hijji Managing Director & Group CISO, E-VASTEL

Trust, Security, and Privacy for Big Data frameworks

12:00pm - 2:00pm, Sep 6

Technical Workshops For Experts

The volume of data in the world is increasing exponentially, also has revolutionized the current digital ecosystem. The readily available large datasets foster AI and machine learning automated solutions. However, the data format and its collection from various sources introduce unprecedented challenges to different domains including IoT, manufacturing, smart cars, power grids, etc., but at the same time highlight the security and privacy issues in this age of big data. One of the serious side effects of the digital age and big data is the growing risk in terms of Trust, Security, and Privacy.

In this regard, Big Data is changing cybersecurity analytics by providing new tools and opportunities for leveraging large quantities of structured and unstructured data. The humongous scale of extraordinary scale, security, and privacy in big data faces many challenges, such as generative adversary networks, efficient encryption, and decryption algorithms, encrypted information retrieval, attribute-based encryption, attacks on availability, and reliability.

In this talk, we will discuss the Big Data system's security layered abstraction (Apache Hadoop stack). This talk involves several essential functions and frameworks, including Identity and access control of the Apache Hadoop clusters, data governance, integrity, confidentiality, and security auditing. Related research areas and associated concepts in data streaming IoT architectures, and cloud will be discussed as well.

Speaker

Feras Awaysheh Assistant Professor, University of Tartu

Be part of the future machine learning and cyber security

12:00pm - 2:00pm, Sep 6

Technical Workshops For Beginners

From Google Trends, machine learning and AI has shown a steady (almost threefold) increase in interest since 2015. In Coursera and Udacity and other platform machine learning courses are both in the top 10 topics. Many people want to learn more about it. AI is “an area of computer science that deals with giving machines the ability to look like they have natural brilliance.” which mean more power in addition to it’s current Power.Systems which are based on AI, sometimes called as cognitive systems, are helping us automate a lot jobs and gear up difficulties which are more complex than most humans are capable of solving. New generations malware and cyber-attacks can be difficult to detect with traditional cybersecurity procedures. What about our current jobs? How we will be impacted? How to avoid this? join me to learn and know...

Speaker

Ahmed Adel Bakr Alderai Cybersecurity Assurance Technical Lead, Telecommunication Company

1:00pm

How Artificial Intelligence Changing Cybersecurity

1:00pm - 2:00pm, Sep 6

Managerial

An organization’s security system may be secure, since it interacts with third parties (customers, regulators,

suppliers, etc.), it is vulnerable through these pathways. According to Accenture, 40% percent of security breaches are indirect, as threat actors target the weak links in the supply chain or business ecosystem. That is why organizations need an automated intelligent solution that can predict attacks and respond quickly.

The basic tenets of AI-enabled programs are that they can collect data, analyze it, make a decision with an understanding of outcomes, and learn from the results. That is why applying AI to cybersecurity brings new defensive promises and offensive challenges to cybersecurity.

Speaker

Ramy AlDamati Co-Founder / Chief Strategy Officer (CSO), AlBrza Full-time

2:00pm

Combatting Payments Fraud in 2021

2:00pm - 3:00pm, Sep 6

Managerial

How to detect the common techniques used by fraudsters and how to mitigate against those attacks

---

Speaker

Mostafa Menessy Co-founder & CTO, PayMob

Role of Digital Signature in Egypt's Digital Transformation

2:00pm - 3:00pm, Sep 6

Technical Workshops For Experts

· Overview on Digital Signature

· Success stories

· Potential projects

Speaker

Eng.Hazem Nabil Vice President, Information Technology Industry Development Agency, ITIDA

3:00pm

Fuzzing: Finding Your Own Bugs and 0days!

3:00pm - 4:00pm, Sep 6

Managerial

This presentation has as objective to explain how 0day are found through Fuzzing technique.
I'll be explaining how you can create a fuzzer, what are types of fuzzers and types of targets.
And how you can find a Buffer Overflow vulnerability, and how to write step-by-step your own exploit.
2 PoC demos included, of course!

Speaker

Rodolpho Concurde Penetration Tester, Independent Researcher

Container Security

3:00pm - 4:00pm, Sep 6

Technical Workshops For Experts

We will go through Container security and the process of implementing security tools and policies that can give you the assurance that everything in your container is running secured.

Speaker

Ahmed Anas Corporate Information Security Manager, EFG Hermes Holding SAE

DFIR Automation Lab

3:00pm - 5:00pm, Sep 6

Technical Workshops For Experts

Illustrating new techniques to perform digital forensics and incident response remotely and automated to facilitate the process of incident response inside any organization.

Speaker

Ahmed Aboalfadl Incident Response and Digital Forensics Engineer, MCS

4:00pm

Moving to the Cloud – Different Security Challenge

4:00pm - 5:00pm, Sep 6

Managerial

Whether people admit or not, everyone is moving to the cloud and all future business will run somewhere on the internet. Cloud security remains top priority where CISOs and CIOs need to think differently to set the new architecture and mindset. More terms are developed and thrown on us each year as CASB, CSPM, CWPP, SASE, Zero Trust and more without clear understanding how they relate to each other and how to position them. This session will try to draw the proper approach to build your cloud security strategy with guidance on new security architecture.

Speaker

Ahmed Nabil Regional Information Security and Risk Manager, Standard Chartered

5:00pm

Challenges to OT Security

5:00pm - 6:00pm, Sep 6

Managerial

The evolving and expanding nature of cyber threats. How do threats look like in future?
The future of connected OT (keeping industry 4.0 in mind) and the threats of the future.
Icebreaker: 5G as tool to hack – One may think that Factory is physically secured very tightly, so no external entity can hack internal Air Gaped wireless network. BUT landing drones on roof of factory is as if Russian/ Chinese Hacker is sitting right on your roof to hack your internal Air Gaped wireless network. In future we might need Radars to detect drones - another dimension of Intrusion Detection. Can't predict where Offensive Security would lead in Prevention of this Intrusion.
IIoT – Industrial Internet of Things: sensors, actuators inviting more threats to OT networks
Consider Smart Cities, Rail, Roads, Stadiums etc. controlled with IIoT especially during Sports Events when whole country under lime light focus of the world while hearing recent (2021) news of OT Cyber Attacks Pipeline Operator in USA, Nuclear Facility in Iran, Power plant in India
Political regional situations igniting threats of Nation State and Activists as well as internal threats of disgruntled ex/ current employees due to Covid related economic situation
RDDOS - Ransom Distributed Denial-Of-Service Attack: Old School Ransomware are still at rise especially because of Bitcoin, but due to billions of cheap less secure IoTs, recently organizations are receiving mails from Threat Actors like: Fancy Bear (APT28), Lazarus, Armada about RDDoS or else their websites/systems will be D-DoSed up to 2Tbps DDoS attack
Threat from the Cyber Supply chain like recent famous incident (SolarWinds)
Securing threats targeting remote workforce
The challenges of the process network keeping remote workforce in mind
Mostly OT Networks should be Air Gapped from Internet or if required should be connected through Data Diode i.e. Unidirectional outbound communication only. Giving access to Remote workforce for OT environment is great challenge, especially for Vendor Support. Following are some Secure Solutions for Remote workforce/ support to meet the challenges:
Jump Servers
Digital Helmet (with camera, mic, headphones...)
Temporary Serial to Internet Connector (with VPN, Firewall etc.)
Remote configuration on isolated replica of production system in IDMZ and then replication of configurations from Replica to Production Systems
Workforce working from homes don't have as many physical, and home network security controls so besides obvious solutions like Virtual Desktop Solutions, MFA - Multi Factor Authentication, VPN, Mobile Device Management (MDM), More focus on End Point Protection (HIPS), EDR- Endpoint Detection & Response, Application Whitelisting and User awareness to be considered.
How the changing nature of cyber-crime and app & data accessibility create risk and the essentials of application and data protection?
The importance of network segregation and robust BCP and DRP.
Remote Work force changed the security landscape totally in competition of providing each and every service to Mobile. This has increased the risks to application and data accessibility as well as privacy related compliance challenges such as GDPR.
But since cyber-crime is expanding it's scope to OT/ ICS environment so beyond risk of data & application now we are facing the risk of loss of human life (the priceless asset), Plant Damage, Plant shutdown, production stoppage, and impacts may lead to much larger in case of cyber attack on critical infrastructure like power/ utility company, oil & gas.
Laying the Foundations for Zero Trust
Segregation again, along with IAM and PAM etc.
Long journey while balancing requirements of Availability especially environments where people work in shifts with shared credentials on legacy systems
Zero Trust with micro-segmentation, least privilege, MFA, IAM, User Behavior Analytics, Machine Learning, AI, Encryption is need of the day against threats like recent Supply Chan Cyber Attack (SolarWinds), Challenges of Remote Work, Insider Threat by disgruntled ex/ current Employees, Contractors as well as Compromised Service Providers. More focus required in cloud environment in terms of Zero Trust
Last but not the least, Zero Trust is not just technology; it's about process and mindset as well
Digital hygiene: Key to outrun cyber threats?
The challenges related to an up-to-date infrastructure/Services and an efficient SNOC.
No silver bullet solution which fits all but top one aspect which return most in majority of the cases is

Visibility.
Visibility of your all information/ IT assets and their importance/ classification
Visibility and clarity of all of your crown jewels
Visibility of all the vulnerabilities of your assets
Visibility and Intelligence of threats to your organization, similar organizations, industry, country
Visibility of your competencies & capabilities
Visibility of traffic, user behavior, machine routine & peak statistics
Visibility of deviations from routines (number of routine attacks/traffic vs abnormally increased number of attacks/ traffic)

Speaker

Muhammad Faisal Syed Senior Tech Engineer, a QP Company

Malware Evolution and their Detection techniques

5:00pm - 7:00pm, Sep 6

Technical Workshops For Beginners

Often computer/mobile users call everything that disturbs/corrupts their system a virus without being aware of what it means or accomplishes. This tutorial systematically gives an introduction to the dierent varieties of samples that come under the broad umbrella known as malware, their distinctive properties, dierent methods of analysing the malware and their detection techniques.
Topics to be covered:
1. Introduction of malware
2. A short history of Malware (virus to malware)
3. Traditional Malware Detection Systems
4. Signature generations
5. 1st Generation Malware
6. Static Malware Analysis
7. Challenges in Static Analysis
8. 2nd Generation Malware
9. Dynamic Malware Analysis
10. Challenges in Malware Analysis

Speaker

Dr. Ashu Sharma Senior Malware Analyst, Watchguard, India

It's Time to Call Your RedTeam

5:00pm - 7:00pm, Sep 6

Technical Workshops For Experts

With the continuous development in cyber attacks, the traditional penetration test has become inadequate, at least it cannot achieve all the desired goals due to the nature of the test, which takes place in intermittent periods and is entrusted with limited goals and vision, so it has become necessary to think from a different angle of view and strive behind Another way to keep pace with this development in cyber attacks and to find innovative solutions commensurate with the development and complexity of hackers' methods, which in turn can protect the largest amount of information.
From here, the idea of adversary emulation exercises has become a necessity, especially since it comes with a completely different mentality from the traditional penetration test, which helps to avoid many faults that the information security team makes and also helps in solving many security holes that the traditional

penetration tester cannot discover. .... And last but not least, it not only requires the discovery of technical vulnerabilities... but it also seeks to discover gaps in the protection method that the information security team follows, which provides us with the necessary information to develop a policy to prevent cyber attacks and deal with them in a manner consistent with the development of methods attack.

Speaker

Mohamed Gamal Cyber Security Senior Consultant, Secure Networks, Egypt

6:00pm

Enabling Trustworthy AI in an Intelligent Digital World

6:00pm - 7:00pm, Sep 6

Managerial

This session explores a Risk Based Approach to AI Cybersecurity and Data Protection based on regional, industry and technology insights and the need for a AI Shared Responsibility Model in the Age of Digital Transformation. The talk explains the risk based approach using use case scenarios looking at various AI deployment scenarios and mapping that to the technology stack for Cloud, Edge and Intelligent Devices.

Speaker

Pat McCarthy AI Security and Privacy Protection Advisor, Huawei

Tue, Sep 07, 2021