The Script Bulletin

JULY 2021

CONTENTS

NEWS

- CREST President, Ian Glover, announces he is stepping down
- CREST becomes 'Founding Member' of UK Cyber Security Council
- CREST GB AGM - election results
- Regional update on regulators and schemes
- CREST Examination Update
- Academic Partners update
- CRESTCon UK 2022 – Save the Date
- CRESTCon UK 2021
- The Case for Continuous Pen Testing
- A look inside this month's NTT Global Threat Intelligence Center: July 2021 Report
- CRESTCon Australia 2021
- New Members
- Events Diary
- CREST Events
- Third-Party Events

NEWS:

CREST President, Ian Glover, announces he is stepping down

After almost 13 years as President Ian Glover has announced that he is stepping down. He will retire from operational work as President of CREST (GB) in three months but will continue to support CREST International projects until the end of the year.

"My retirement is something I have been planning for some time and, while I leave with a heavy heart, I am confident CREST will continue to move forward in the hands of an excellent team," said Ian, making the announcement at the CREST (GB) AGM on 17 June. "Over the last 13 years at CREST I have tried to give back to the community that I have worked with for over 40 years. I sincerely hope I have helped organisations to mature and grow and encouraged individuals to enter and thrive in an increasingly professional industry."

During nearly 13 years at CREST, Ian has elevated the not-for-profit organisation to become a global influence in the cyber security industry. He has positioned it as thought leader and innovator in technical cyber security assurance. He has also been instrumental in many major government and industry initiatives to improve cyber resilience.

"On behalf of the CREST (GB) Executive I would like to thank Ian for everything he has done for CREST members and the cyber security industry," said Rob Dartnall, Chair of CREST (GB). "As president, he has transformed CREST and he can be very proud of the work he has done to develop and professionalise our industry. Truly a legacy to be proud of."

Making his announcement, Ian stressed that his exit was being planned in a very controlled and structured way to ensure that there would be no adverse effect on CREST. He also took the opportunity to thank everyone who had supported and helped him over the years.

Ian also spoke about his decision to step down in his closing address at CRESTCon UK on 29 June, which you can watch here:

https://youtu.be/uBtM-9ls8-M

CREST Events

CREST Workshops

Industry Events

NEWS:

CREST becomes 'Founding Member' of UK Cyber Security Council

CREST has been awarded 'Founding Member' status of the UK Cyber Security Council. This is a reflection of CREST's work to set up the Council alongside the other members of the Cyber Security Alliance – the group of organisations that were originally commissioned by DCMS.

"Being awarded 'Founding Member' status is permanent acknowledgement of the significant contribution that CREST and the other 15 organisations involved in the Cyber Security Alliance have made to help get the Council off the ground," Ian Glover, President of CREST commented. "CREST looks forward to working closely with the Council in the future to further develop and grow the cyber security profession".

The UK Cyber Security Council (**https://www.ukcybersecuritycouncil.org.uk/**) is the self-regulatory body for the UK's cyber security profession. It develops, promotes and stewards nationally recognised standards for cyber security in support of the UK Government's National Cyber Security Strategy to make the UK the safest place to live and work online.

CREST GB AGM - election results

CREST is pleased to announce the election of Rodrigo Marcos Alvarez (SECFORCE Ltd), Brian McGlone (IBM UK) and Boglarka Ronto, (Commissum Associates Ltd) to the CREST GB Executive at the AGM that took place on 17 June. "On behalf of everyone on the CREST GB Executive I would like to congratulate Boglarka, Brian and Rodrigo," said Rob Dartnall, CREST GB Chair. "Being elected by the CREST Membership is a reflection of the important work and contribution they will be able to make to CREST by representing and reflecting both member and industry interests. Thank you to everyone who stood for election, everyone who attended the AGM and to everyone who voted either on the day or by proxy."

Mark Turner, NCC Group, retired by rotation at the AGM after serving six continuous years on the CREST GB Executive. John Fitzpatrick, who was eligible to stand for re-election having served three years on the Executive, decided not to stand. Everyone at CREST would like to thank Mark and John for the time and commitment they have given to CREST over the years.

Regional update on regulators and schemes

CREST engages internationally with government bodies, regulators and key stakeholders. Below is a list of these that CREST has been engaging with. CREST promotes its line of certification, and company accreditation including its member companies.

Europe

- CBEST – Bank of England/PRA
- GBEST – UK Cabinet Office
- CHECK – NCSC
- CIR - NCSC
- ASSURE – Civil Aviation Authority
- TBEST - Ofcom
- TIBER – ECB
- ENISA
- IATA – International Air Transport Association
- Physical Penetration Testing – UK Cabinet Office
- International Trade Missions – Department for International Trade
- FCDO – Foreign, Commonwealth & Development Office

Asia

- HKMA – iCAST
- MAS & CSA
- State Bank of Pakistan
- Bank Indonesia
- Bank Negara – Central Bank of Malaysia

Australasia

- CORIE – Australia's Council of Financial Regulators
- Aviation

The Americas

- Center for Internet Security
- CMMC
- NSCAP CIRA
- DHS
- DoD
- Bank of Canada

Continued over >

NEWS:

Middle East

- DESC – Dubai Electronic Security Center
- CITRA Kuwait – Communications & Information Technology Regulatory Authority
- Israel National Cyber Directorate
- MOTC Qatar – Ministry of Transport & Communications

International

- GFCE - Global Forum on Cyber Expertise
- WEF - World Economic Forum
- World Bank

If you would like any further information on any of the above schemes and regulators in then please contact **samantha.alexander@crest-approved.org**.

If members feel there are any organisations missing from the list that they would like CREST to engage with, then please also contact Sam: **samantha.alexander@crest-approved.org**.

CREST Examination update

CREST practical examinations reopened in the UK on 15 June 2021, after the COVID 19 compulsory closures, and are currently being held in 3 locations: Heathrow, Cheltenham and Milton Keynes. Dates and locations of examinations can be found on the Examination Update on the CREST website: **www.crest-approved.org** To book examinations or for more information, please contact **exambookings@crest-approved.org**.

Pearson Vue Centres in the UK reopened on 12 April and although they initially had a few capacity issues due to the backlog of candidates following lockdown, this now seems to have been sorted out and consultants wishing to book CREST theory examinations shouldn't have any problems. **www.pearsonvue.com/crest**. For the rest of the world, please check the following link for more information on the relevant regions: **https://home.pearsonvue.com/coronavirus-update**.

Academic Partners update

Over the last few months CREST has held three really constructive skills-focused workshops with its Academic Partners and its Penetration Testing, Incident Response and Threat Intelligence focus groups. A big thank you to everyone who was able to attend and contributed to these initial discussions. We found that while there were some elements unique to the disciplines, there were also a number of elements that were common across all of them – such as the need for more visibility of real world experience.

If anyone would like to have a copy of the notes from these workshops then please contact **allie.andrews@crest-approved.org**

CREST is planning to hold an event for cyber security students on 3 November that will give them an opportunity to learn from CREST Qualified Individuals about their careers, watch technical presentations and ask questions in a quick-fire mentoring session. More information on this will be available soon but please email **marketing@crest-approved.org** if you are interested in presenting or attending.

CREST is also putting together an informal working group across the Penetration Testing, Incident Response and Threat Intelligence disciplines to look at the actions from the previous workshops. If you are interested in taking part then please contact **adriana.costa-mcfadden@crest-approved.org**. The first meeting will take place in mid August.

CRESTCon UK 2022 - save the date

We are looking ahead to next year's event, which is booked for 12 May 2022 at the Royal College of Physicians. Very much looking forward to seeing you there.

NEWS:

CRESTCon UK 2021

CRESTCon 2021 took place on 29 June as a virtual event. Thank you to everyone who presented, attended and who helped to make the event a success. While it was a shame we couldn't run it as a physical event due to Covid restrictions, we were still able to deliver three streams. For those who missed the event or particular sessions, most of the content, is now available on the CREST YouTube Channel – **www.youtube.com/crestadvocate**

Thank you very much to our Gold Sponsors Titania and NTT. A big thank you also to our other sponsors PwC, Foregenix, Obrela Security Industries, Bob's Business, Security Alliance, JUMPSEC, Nettitude, ICSI, Media 7 and our community sponsors.

Plenary sessions

WELCOME:
Ian Glover, President, CREST

Watch here:
https://youtu.be/KDVDGcWIUa8

KEYNOTE:
Tracy Buckingham, Deputy Director Security and Cyber Security Exports, Department for International Trade.

UKDSE A UK Government Perspective on Cyber Security

Watch here:
https://youtu.be/gkj6UwktGb4

Stream 1 – Penetration Testing

Aleksander Gorkowienko,
Senior Managing Consultant, Spirent Communications

SCADA/ICS Security AD 2020 – Do We Learn From Our Mistakes?

Watch here:
https://youtu.be/py3Tkg1_ucM

Matt Lorentzen,
Principal Consultant, Cyberis

Click Here for More Information

Watch here:
https://youtu.be/OzkzHoa34V4

Ken Munro,
Partner, Pen Test Partners

The whistle-stop tour of aviation security

Watch here:
https://youtu.be/AAK9gXy_Ip4

Keith Driver,
CTO, Titania

The value of continuous auditing in Zero Trust architecture and risk-based situational awareness

Watch here:
https://youtu.be/MtIfGgAvZQI

Rupert Collier,
VP Sales EMEA/APAC, RangeForce

The pitfalls, gotchas and recipes for success in building high quality Red Team Exercises

Watch here:
https://youtu.be/ACKPThg9g40

Nigel Thorpe,
Technical Director, SecureAge Data Centric Security

Watch here:
https://youtu.be/THeaNPlnEm0

Costas Senekkis,
Penetration Testing Team Lead, ICSI Ltd

apt-get CREST CPSA/CRT

Watch here:
https://youtu.be/fNwVzBPKwNo

>>

NEWS:

Stream 2 - Threat Intelligence

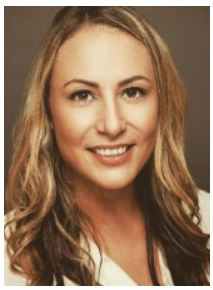
Mark Vaitzman,
Senior cyber security analyst

Nethaniel Ribco,
Senior cyber threat intelligence analyst, CyberProof

The Inner Workings of Cyber Defenders

Watch here:
https://youtu.be/svj9yy5P9MA

Dr Jamie Collier,
Cyber Threat Intelligence Consultant



Rebecca Simpson,
Senior Intelligence Enablement Manager, FireEye Mandiant

I Can't Get No Stakeholder Satisfaction - Optimising Feedback in the Intelligence Lifecycle

Watch here:
https://youtu.be/LZ1N3BAkPbI

Laveena Shetty,
Cyber Threat Detection & Response Analyst, BDO UK LLP

Open Source Intelligence (OSINT) and its use in Incident Investigation

Watch here:
https://youtu.be/p9flodElRIY

Karla Reffold,
COO, Orpheus Cyber

The importance of threat intelligence in monitoring your third party risk

Watch here:
https://youtu.be/NvjknzfusKU

Robert A. Moody,
Cyber threat intelligence and digital forensics expert, The Home Depot

The threat lurking in the shadows

Watch here:
https://youtu.be/LIEEcFlkax8

NEWS:

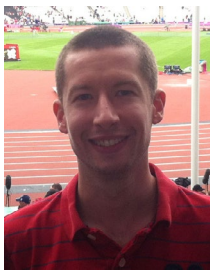
Stream 3 – Incident Response & Awareness

Alan Melia,
Principal Investigator

Mehmet Mert Surmeli,
Senior Incident Response Consultant, F-Secure

Flying by the seat of your Pants!

Watch here:
https://youtu.be/GBbNSSI43RQ



Andy Snowball,
Head of Incident Response, BAE Systems

2020 – A Year of Ransomware

Watch here:
https://youtu.be/vl71IFAhvWE

David Gray,
Director, Security Consulting – Global DFIR, Security Operations Consulting, NTT Ltd

Cybersecurity Survivorship Bias – Avoiding it and where to put your armour

Watch here:
https://youtu.be/CNwMp-fbH9A

Tom Hall,
Head of Blue Team, 6point6

How purple teaming can prepare an organisation for ransomware breaches

Watch here:
https://youtu.be/K4vu6BtU6QE

Luke Price,
Senior Technical Consultant

Sean O'Connor,
Senior Technical Consultant, CYSIAM

SOC to IR, am I ready?

Watch here:
https://youtu.be/5UuQxmALGqM

Richard Hollis,
CEO, Risk Crew

Cybercrime.com – The Org Chart

Watch here:
https://youtu.be/f1nzYwz-nfc

Sarah Janes,
Owner & Founder, Layer 8

From Compliance to Culture Change: how a little bit of science goes a long way

Watch here:
https://youtu.be/UFroduy5iR8

>>

NEWS:

CRESTCon Sponsor article

The Case for Continuous Pen Testing

Penetration Testing in some shape or form has been around since the 1960s, coming to the fore in the 1980s, when the US Navy began to deploy pentesters to check the security posture of its systems. The military is still setting the standard today when it comes to cybersecurity and it mandates its supply chain to take the same rigorous approach to security, hence the new CMMC risk management framework for the Defense Industrial Base.

While of course technology as a feature of our everyday business and personal lives has rapidly evolved since the 1980s, designing systems to "keep the bad guys" out remains a fundamental principle of network security. However, as the technology evolves and becomes more sophisticated, so does the attackers' tool-set.

Taking the 'Walled Garden' approach - e.g. placing our most valuable assets in the middle of our layers of defense and crossing our fingers (!) - is no longer enough. Gone are the days of Red Teaming as an annual activity or perimeter/network node testing, if and when the internal team has the time. Networks change daily. So continuous testing of defenses needs to be a core part of your cybersecurity planning.

The Crumbling Walls

Sadly, the sharing of best practice and knowledge among those working in cybersecurity, intended for genuine, fellow professionals to benefit from, also falls into the hands of attackers. With Cyber Security standards and vulnerability databases for different sectors and jurisdictions easily accessible via a quick desktop search, hackers have a blueprint to plan their next attack. Even more worryingly, free tools designed to aid attacks are readily available on the internet and many don't even require a particularly high level of skill to deploy.

The other advantage attackers are benefitting from is that the wall itself, or the network perimeter, has become blurred. Even before the pandemic, dynamic, virtual networks to enable consumers to interact with brands 'on-the-go' and for people to work from anywhere, anytime, were becoming mainstay. However, where previously this evolution could be planned carefully by organizations with security in mind and a step-by-step approach taken, the pandemic bought about the need to quickly get people connected in a whole raft of locations using a number of different networks and BYO devices.

Obviously, just the speed at which this had to happen (pretty much overnight in many cases), for businesses to keep functioning, raised the cyber risk organizations are now tolerating. Where a more methodical, security-first approach may have been taken previously, the very real financial need to keep things running came first, along with the rapid deployment of SaaS applications and complex, API-driven services.

As headlines go to show, even McDonald's, despite reporting 'substantial investments' in cybersecurity measures, recently experienced a serious data breach, with customer and employee's personal information being exposed in South Korea and Taiwan.

In North America, earlier this month, 3.3 million Volkswagen and Audi customers' details were compromised, including highly sensitive information such as social security and loan numbers in some cases. Aside from the cost of reputational damage, Volkswagen is having to provide credit protection and $1 million of insurance against identity theft to those who were among the 90,000 customers most seriously affected.

Indeed, most organizations' defenses are not impenetrable.

So what's the answer?

To meet the needs of the ever-changing organization, there understandably needs to be flexibility in your network perimeter as requirements and business priorities change. But not all enclaves should be accessible to everyone. This is why network segmentation has never been more vital. And why DISA (The Defense Information Systems Agency) recommends a Zero Trust Architecture (ZTA) where organizations' focus on segmentation to continuously harden the perimeter of their most valuable services and assets, or 'protect surface'.

The Zero Trust (ZT) approach ***assumes*** compromise of the network – aiming to make it as hard (and expensive) as possible for attackers to move laterally by ensuring every access is authorized by verification and authentication of the user, device type, location, and network.

"The intent and focus of Zero trust frameworks is to design architectures and systems to assume breach, thus limiting the blast radius and exposure of malicious activity," explains Brandon Iske, DISA Security Enablers Portfolio Chief Engineer.

DISA Portfolio Manager, Security Enablers Portfolio, Joseph Brinker continues:

[ZT] is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verifying once at the perimeter to continual verification of each user, device, application, and transaction.

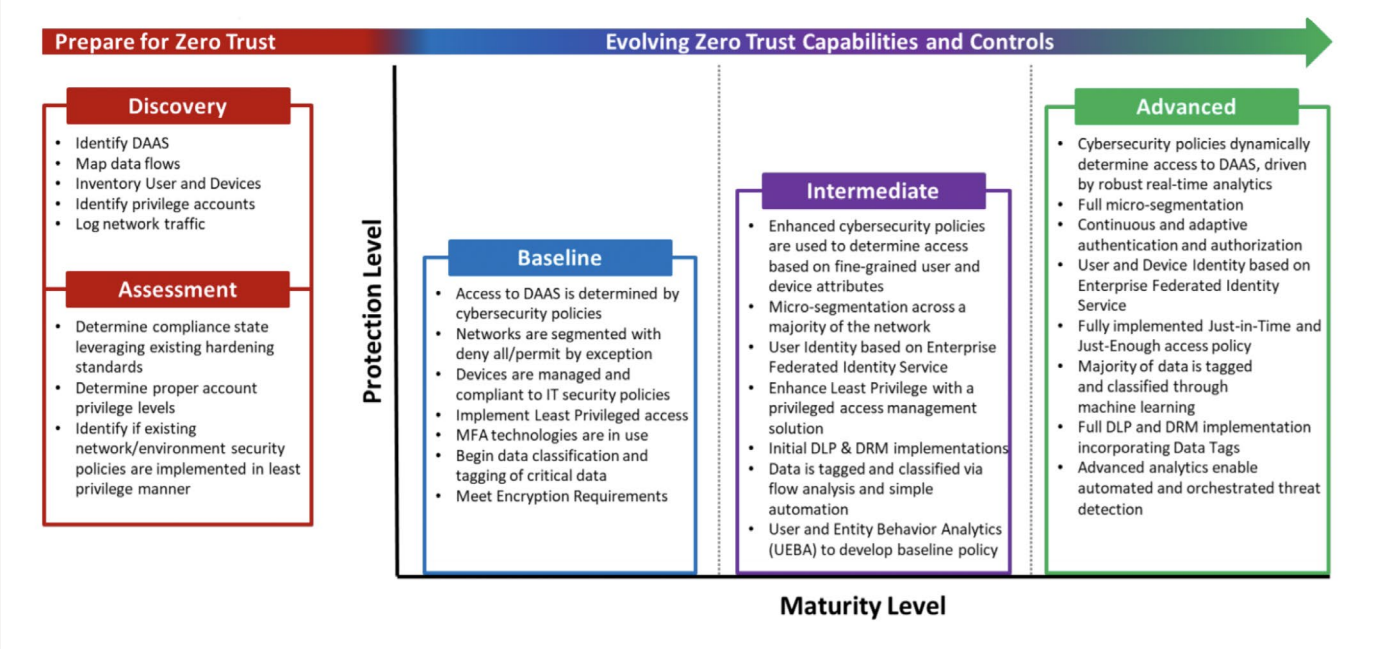
ZTA is simply not possible without adequate security automation.

>>

NEWS:

Security automation in action

To help get started on the road towards developing a Zero Trust framework, DISA has helpfully developed this pathway to migration.



Unsurprisingly, Discovery and Baselining are crucial first steps in this process, as without getting the basics right it's impossible to build a strong foundation for more complex security measures to flourish. You have to know your network. And you have to test its defenses. Conducting a Pentest at the start of the process and repeating it a year later is not enough. And it's not about testing a sample of the network regularly either; you need to be testing every device, every day and continuously mitigating the risks you find.

Most organizations that deploy Pentesting and Network Auditing successfully use automation tools already – such as Titania's Nipper for accurately auditing core network devices. But to automate daily device audits, particularly in large organizations, the tools you use ideally need to be integrated into your enterprise stack and the results aggregated in your SIEM. This is why Titania has developed Nipper Enterprise, harnessing 25 years of pentest and configuration management expertise in a solution capable of auditing hundreds of thousands of firewalls, switches and routers on an hourly basis.

Crucially, our software gives visibility not only to vulnerabilities and misconfigurations, but assesses the ease and impact of exploitation and the ease of fix as well. It then provides remediation recommendations and exact technical fixes to address each issue - delivering continuous risk and remediation prioritization. You can also apply a compliance lens to your network with Nipper Enterprise's dashboards and reports to provide continuous assurance against a range of risk management frameworks including CMMC, NIST 800-171/53 and PCI DSS.

So, if you're preparing for ZTA (and let's face it, we should all be aiming for this!), the case for continuous pentesting is clear. The first step to achieving it is in choosing security automation solutions that give you the foundations for accurate and continuous risk remediation, in order to free up the valuable time of your experienced security professionals. Enabling them to focus on bigger ticket issues at play and the more complex elements of achieving a Zero Trust Network.

Network Penetration Testing Tools from the Experts - Titania

Contact: **enquiries@titania.com**

>>

NEWS:

CRESTCon Sponsor article

A look inside this month's NTT Global Threat Intelligence Center: July 2021 Report

According to the 2021 Global Threat Intelligence Report, the volume of attacks targeting the manufacturing industry increased by nearly 300 percent from 2019. This is due to several reasons related to evolutions in the manufacturing industry and increased adoption of OT-related technology. Other contributing factors were the increased complexity in manufacturing organizations, such as complex supply chains, and the decrease in those organization's security maturity.

The July 2021 Monthly Threat Report summarizes how important a planned strategy for backup and recovery can be to support an organization's Industrial Control System (ICS)/Operational Technology (OT) environment. Though an OT system often does not function exactly like a standard IT environment, some of the same rules apply to the management of each. And, implementation of an effective backup/restore strategy can be crucial to ensure an organization is able to restore their OT environment in the shortest time possible. This includes identifying what parts of the ICS environment are key, and which parts can be backed up/restored.

The July report also looks at continuing research by NTT, including recently published white papers on both Grim Spider and ENT-1. Grim Spider is part of the Wizard Spider threat actor group, and is widely associated with Trickbot infections finishing with the Ryuk ransomware. ENT-1 is also known as the Winnti Group. ENT-1 is highly active and runs multiple parallel operations primarily targeting entities in Asia. New research suggests they are a well-funded threat actor group who makes extensive use of scanners and toolsets such as the Winnti backdoor. Both these groups continue to be active.

Additionally, this monthly threat report features a quick summary of the Summer Olympics Threat Assessment recently published by the Cyber Threat Alliance in April 2021. NTT contributed to the report, which identifies various threats against the Games. According to the report, the top three attacks most likely to be directed at activities around the Olympics are nation-state cyberattacks, ransomware attacks, and disruptive/disinformation attacks. Hostile activities are expected to begin prior to the Games, and continue after in attempts to disrupt the Games and compromise organizers.

Resources
Are you looking for visibility of high-priority emerging threats and vulnerabilities? Take a look at our Emerging Threat Advisory service here.

Visit us at: **https://hello.global.ntt/**

CRESTCon Australia 2021

The inaugural CRESTCon Australia took place as a physical event on 8 April with an excellent line up of speakers. Events like this would not be possible without the support of sponsors and partners. So, a big thank you to Infotrust, Privasec, Triskele Labs, The Canberra Convention Bureau, APAC CIO Outlook and also all the student volunteers, staff at CREST and PRPR that have worked so hard to help make it a success. A special thank you also to Triskele Labs for sponsoring the networking drinks. We look forward to welcoming everyone back for CRESTCon Australia 2022 and hope to be announcing the date very soon.

Most of the videos of the presentations are available on the CREST YouTube Channel – **www.youtube.om/crestadvocate**.

Michal Knapkiewicz, Manager, Advanced Security Centre, EY

Breaking out of restricted Unix shells

Watch presentation here:
https://youtu.be/XdZh5st6Vww

Watch interview with Michal here:
https://youtu.be/Bx_EGMn5Nzg

Nadeem Salim, Principal Security Consultant, NCC Group

Adversary simulation in modern environments

Watch presentation here:
https://youtu.be/e5HpyGGIAq0

Benjamin McMillan, Senior Consultant, Privasec

The benefits of Infrastructure as Code for adversary simulation

Watch presentation here:
https://youtu.be/1G50zlCwIcY

Watch interview with Michal here:
https://youtu.be/6msZQWHeLrk

Chathura Abeydeera, Associate Director, KPMG

How to conduct an effective red and blue team exercise

Watch presentation here:
https://youtu.be/L-3jdah0M0s

Watch interview with Michal here:
https://youtu.be/Sirv1kEFS60

Edward Farrell, Director, Mercury ISS

Monitoring the monitors: a path to keeping the SOC in check

Watch presentation here:
https://youtu.be/VMlUsnTtlm4

>>

NEWS:

New members

Organisation	
	**S-RM Intelligence and Risk Consulting Ltd** S-RM is a global risk and intelligence consultancy. Founded in 2005, we have 250+ experts and advisors across 6 international offices. Headquartered in London, we have offices in Cape Town, Hong Kong, New York, Rio, and Washington DC. We provide intelligence that informs critical decision-making and strategies, from investments and partnerships through to disputes. We help our clients exploit opportunities and navigate complex risks globally. We make organisations more resilient to cyber, operational and security threats. We work alongside our clients to assess, design and implement effective risk mitigation plans. We respond to cyber attacks, security incidents, and organisational crises. We partner with our clients to rapidly contain incidents and crises, understand root causes, and help them to recover quickly.
	**Nexon Asia Pacific Pty Ltd** Nexon delivers cutting-edge, boundary-pushing interconnected solutions that enable your dynamic business to run more efficiently, create better user experiences, and explore bigger and better opportunities. With our customers at the centre of our operations, we help clients run their business better, acting as an integral part of their team in all I.T. matters. From Security to network, cloud services, unified communications, business solutions, digital workspace, right through to desktop and day-to-day support, we take the necessary steps to transform an organisation, enabling sustainable growth and pathways for innovation.
	**Sentrium Security Ltd** Sentrium was founded with the belief that cyber security services should be straightforward and tailored to the needs of our clients. We work tirelessly to help businesses address their security challenges and understand how they are at risk from the ever-changing threat landscape. Our collective knowledge and broad range of high-quality services ensures that we can provide comprehensive assessment solutions and cyber security consultancy to businesses of all sizes, across a diverse range of industries. Our team has extensive experience in providing security services, having worked across all major market sectors, including finance, retail, manufacturing and technology. We take pride in our collective technical expertise and breadth of skills, which enables us to work with all major enterprise technology platforms and a broad range of specialist disciplines.
	**Ruptura InfoSecurity Ltd** We are a boutique cyber security company, specialising in providing penetration testing and offensive cyber security services to the UK market. Our team have extensive offensive cyber security experience and have worked with a large variety of clients both in the public and private sector. We pride ourselves on the quality of our work and the level of technical expertise that we can offer to our clients. We specialise in penetration testing, but also offer various accreditations such as Cyber Essentials, Cyber Essentials Plus and PCI-DSS compliance. Our aims are to maintain our high standards of service and to stay one of the 'go-to' organisations for specialist, in-depth penetration testing solutions.
	**Secora Consulting Ltd** Secora Consulting is focused on forming long lasting partnerships to assist you with your cyber security requirements. We understand the challenges of security testing and keeping your business secure. Our goal is to improve your cyber security operations, providing peace of mind in an ever-evolving threat landscape. As your trusted security partner, our team will provide you with our extensive knowledge from working in high risk, sensitive environments. We partner with high profile multinational corporations, SME's, government departments and public sector organisations in Ireland and throughout Europe. We are trusted by all our partners as our team only consists of highly qualified, security consultants who are experienced and passionate about cyber security. This is reflected by the number of industry recognised certifications within our team. We use our experience and consistent methodology to highlight any failing security controls and underlying issues to help protect your systems and reduce overall risk.

NEWS:

New members

NRI Secure Technologies Ltd

NRI SecureTechnologies Ltd. is a recognized leading security services provider that was created in 2000 as a subsidiary of the Nomura Research Institute (NRI) a company whose 50-year history includes such highlights as being Japan's first private think tank and the installation of Japan's first commercial computer system. Today, specializing in cybersecurity and recognized as a leader in advanced managed security services, penetration testing, and security consulting, NRI SecureTechnologies is focused on delivering high-value security outcomes for our clients with the precision and efficiency that define Japanese quality.

Civica

Civica provides a wide range of solutions for the public sector and regulated private sector markets around the world.

CovertSwarm Ltd

Founded in 2020, CovertSwarm exists to continually out-pace the cyber threats faced by its clients using a constant cyber attack methodology that blends modern penetration testing, red teaming with clientbespoke research and development. Through our continuous offensives against our client's entire organisational asset-base (people, process, procedures and physical) we close the cyber risk gap that exists between more legacy forms of 'point in time' cyber testing. Employing full time ethical hackers, and underpinned by our 'Offensive Operations Centre' portal, CovertSwarm's clients gain rapid value from our continuous approach to improving their cyber security posture as we emulate APTs and nation-state levels of covert attack. We believe in educating our clients on matters of cyber security and 'giving back' to the cyber security community through regular posts, presentations and other information/finding disclosure.

Arculus Ltd

Arculus is a specialist provider of cyber security consultancy, testing and compliance services to public and private sectors. Arculus provides penetration testing services to clients supporting identification and understanding of security vulnerabilities and advising on suitable technical action to address them. Testing is carefully scoped to ensure maximum return on investment. Testing is carried out by qualified and experienced consultants. Recommended remediation measures are pragmatic and prioritised supporting real improvement to the overall security posture of the organisation.

Crowe Global

The public expects you to have a digital presence – and to keep their data secure. You can take the appropriate precautions, but there will always be risk. That's why how you respond to an incident is just as important as trying to prevent one. Having the right cybersecurity program in place for your organization is crucial. Crowe can help you protect the right areas of your organization with the right resources by finding gaps and helping to redesign or implement improved safeguards to your cybersecurity program.

SISA Information Security Pte Ltd

SISA is a global Payment Security Specialist, trusted by organizations across the globe for securing their businesses with a robust preventive, detective, and corrective security services and solutions. SISA is a recognized PCI QSA, PA QSA, PCI ASV, P2PE-QSA, 3DS Assessor, PCI Forensic Investigator, and PCI PIN Security Assessor and has a comprehensive bouquet of advanced products and services for risk assessment, security compliance and validation, monitoring and threat hunting, as well as training for various payment security certifications. SISA currently services 2000+ clients spread across 40+ countries through our delivery centers in the U.S.A, U.K, Bahrain, U.A.E, Saudi Arabia, India, Singapore, and Australia. Our clientele spans industries ranging from banking, financial services and insurance, retail, airlines, hospitality services, e-commerce merchants, payment gateways and service providers, BPO & call centers, card personalization & processors, and IT & ITES companies, etc

Fortbridge

This is a family business, started by two brothers, highly skilled and with more than 20 years of experience in the security industry. Reach out and we will tell you more about what we do and how we do things differently.

>>

Events Diary

EVENTS Diary:

Month	Event & Location	Type	Date	Year
Aug	CREST SOC Focus Group	Virtual Meeting	02 Aug	2021
Aug	CSIR Focus Group Meeting	Virtual Meeting	12 Aug	2021
Aug	Journey to the center of cloud: The essential approach to governance and security in the post COVID era, ST Engineering	Webinar	17 Aug	2021
Aug	Content management systems and the importance of vulnerability management, Responsible Cyber	Webinar	17 Aug	2021
Aug	CREST Penetration Testing Focus Group Meeting	Virtual Meeting	24 Aug	2021
Sep	National Cyber Security Show – NEC Birmingham	3rd Party Physical Event	07-09 Sep	2021
Sep	CREST Access to Cyber Security Event	Virtual Event	22-23 Sep	2021
Sep	CREST Threat Intelligence Professionals (CTIPs) networking drinks reception	Physical Event	30 Sep	2021
Nov	Academic Careers Pathway Event	Virtual Event	03 Nov	2021
Nov	CREST Fellowship Ceremony	Physical Event	11 Nov	2021
Nov	Accreditation Webinar – New members	Virtual Event	18 Nov	2021
Nov	CREST Threat Intelligence Professionals (CTIPs) committee & assessors	Virtual Event	TBC	2021
Dec	CSIR Focus Group Meeting	Virtual Event	06 Dec	2021
Dec	CREST Threat Intelligence Professionals (CTIPs) networking drinks reception	Physical Event	09 Dec	2021
Dec	Meet the CSIR committee panel	Virtual Event	TBC	2021
Mar	CREST Threat Intelligence Professionals conference	Physical Event	03 Mar	2022
Apr	CRESTCon Australia	Physical Event	TBC	2022
May	CRESTCon UK	Physical Event	12 May	2022

Events Diary

CREST Events:

CREST SOC Group Online meeting, 2 August, 9am – 10:30am BST

The next meeting of the SOC Focus Group will take place over the 'Microsoft Teams' platform. Members, please contact **marketing@crest-approved.org** to be added to the calendar invite.

CSIR Focus Group Online meeting, 12 August, 11am – 12pm GMT

CSIR Focus Group will take place over the 'Microsoft Teams' platform. Members, please contact **marketing@crest-approved.org** to be added to the calendar invite. Thank you to everyone who has participated in the meetings already, and for all of the feedback received.

CREST Penetration Testing Focus Group online meeting, 24 August, 10am – 11.30am GMT

CREST Penetration Testing Focus Group will take place over the 'Microsoft Teams' platform. Members, please contact **marketing@crest-approved.org** to be added to the calendar invite. Thank you to everyone who has participated in the meetings already, and for all the feedback received.

CREST Access to Cyber Security Event – 22-23 September, 08:00-17:00 BST

2 days of workshops and webinars focused on ensuring careers in cyber security are made accessible to everyone. There will be a number of workshops that will all aim to educate and offer constructive advice and guidance for both employees and employers. Topics will include stress and burnout; neurodiversity; gender balance, physical disability, CV writing and socio-economic status & career development. If you have any queries or suggestions for webinars then please contact **marketing@crest-approved.org**.

Events Diary

CREST Events:

CTIPS Networking Drinks Reception – 5pm-10pm, 30 November, Venue TBC, London

The CTIPS (CREST Threat Intelligence Professionals) group is holding a networking drinks reception on 30 November in London. CREST will provide drinks and canapés and chance to network with other Threat Intelligence professionals. If you are interested in attending please contact **marketing@crest-approved.org** for details.

CREST Fellowship Ceremony and Dinner 11 November 2021, Royal College of Physicians

Announcing the CREST Fellowship ceremony and dinner date for 2021. Keep watching for the tickets to go on sale. If you have any questions, please email us at **marketing@crest-approved.org**

Learn about CREST Company Accreditation – 18 November, 08:00 & 16:00 GMT

In this webinar CREST's Principal Accreditor, Samantha Alexander, will provide an update on CREST Accreditations and information on the process of becoming an Accredited Company. There will also be an opportunity to ask her any question you may have on the accreditation process. Questions can be sent in advance to **marketing@crest-approved.org** or you can ask them on the day via the question panel.

Coming soon: Meet the IR panel & CTIPs Committee panel. If there is a panel subject that you would like us to schedule please contact **marketing@crest-approved.org** with your suggestions or any other suggestions for webinars.

Events Diary

CREST Events:

CREST Partner Events:

National Cyber Security Show (NCSS) : NEC Birmingham – 07-09 September 2021

The event was developed with support from a group of the industry's major players to deliver a world class exhibition dedicated to UK security professionals, installers and integrators, providing opportunities for direct engagement across the supply chain.

There is a tailored education programme that investigates the evolving challenges and opportunities involved in the delivery of security projects throughout the supply chain. The Security Event will tap into the expertise of leading security professionals and explore the latest innovations from suppliers.

https://www.thesecurityevent.co.uk/National-Cyber-Security-Show

NCSS is offering CREST member companies a 10% discount on sponsorship. If you are interested please contact Heike: **marketing@crest-approved.org**