Q3 - 2022 ISSUE

ISACA
Bangalore Chapter

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

CONTENTS

ISACA Bangalore Chapter

InfocITy Auditor

Q3 - 2022

From The Desk Of The President

Dear Members,

Greetings of the day to you!!!

We had an overwhelming response and participation for our 25th Annual Karnataka Conference – our silver jubilee edition with the theme "**People, Technology and Evolving Security – An Eventful Triangle"** which was held on the **29th & 30th of July, 2022** between 9:00am-6:00pm. We returned to the in-person conference after two full years of gap due to pandemic. We wanted to make it more meaningful and valuable for our Members and hence for the first ever time we engaged the Event Management team in supporting us to conduct the Annual Conference. The Conference was very well accepted by all the Members who participated shared loads of positive feedback.

We represented ISACA Bangalore Chapter and actively participated in the International Community Day which was scheduled on the 1st of Oct 2022. We had a good response coming in from our Members and a lot of our EC Members participated in this event, where we visited the "So Care" NGO and met the kids and spent some quality time with them along with giving them some insights and awareness on Cyber Security and by distributing some sports gears.

Building Committee was able to finalize on a Building for our ISACA Bangalore Chapter which was a long awaited achievement. We presented the detailed report to our Members in our Special General Body Meeting held on the 15th of Oct at Pride hotel, Richmond Circle, Bangalore. We had an overwhelming response of 60+ Members participating in the meeting who made it a very interactive session. The Committee approved the New Building unanimously. We will be proceeding with the registration process post submission of certain documents that was agreed upon in the SGM.

It is that time of the year where we would be meeting as a team to go over the entire year's performance and plan some of the new requirements that would help our Chapter's growth. Yes, we are referring to the Annual General Meeting (AGM) which is scheduled to take place on the 29th of Oct 2022. We are looking forward to meeting you all and taking the inputs and suggestions on the way forward and also glad to seek your support in helping us to elect the new Executive Committee for 2022 - 2023.

This year was filled with loads of activities. We have tried our best to get maximum value add our Members. We had conducted series of virtual and in-person events on:

- Intro Seminars
- CPE Meets
- Review classes
- Short Learning Bytes (SLB)
- Amendments to the By-Laws
- Closure on the New Building

My sincere thanks to all the Members and the colleagues in the Executive Committee for providing excellent support in the entire Chapter related activities. I was fortunate enough to continue as the President of ISACA Bangalore Chapter for two consecutive years. I take pride in saying that our Chapter elevated to the largest Chapter of India and was able to maintain the same at that top level for two consecutive years and I am sure my successors will strive towards maintaining the same. The current team will sign-off post the AGM and the new team will be in place for the next term starting 29th of October 2022.

Looking forward to meeting you all at the Annual General Meeting!!!!!

Stay Safe and Stay Healthy!!!!!

Regards,

VELMURUGA VENKATESH, CRISC, CDPSE, COBIT-5 (F), ISO 27001 LA, ISO 31000 CRM
President

Message From the Vice President

Dear Friends,

Greetings.

As the country returns to normalcy post-COVID, we have all started spending a lot more time outside our homes. Considering this we had planned for an in-person Annual conference after two years.

We had a fantastic silver Jubilee edition 25th ISACA conference held in person on 29th & 30th Jul 2022 at Sterlings Mac Hotel. The theme was **'People, Technology and evolving Security...An eventful triangle'.** I believe most of you have attended and those who have missed, watched the recorded session hosted on our YouTube channel.

The conference was attended by more than 220 delegates. Mr. Pratap Reddy, IPS Commissioner of Police, Bengaluru City Police was the Chief guest and inaugurated the Annual Conference. Dr. Aloknath De, Exec Consulting Director-Samsung India, Adjunct Prof-IISc, Bangalore was the Keynote speaker for first day. Mr. Sunil Panwar, IFS Chief Executive Officer, Center e-Governance, Government of Karnataka was the keynote speaker for the second day. We had several speakers from various sectors of industry from India and abroad presenting a variety of topics that emerged on conference Theme. Delegates shared excellent feedback for our first in-person annual conference post-COVID. ISACA BC will continue to engage various government bodies in the future for sharing best practices and knowledge-sharing sessions**.**

As part of community day on Oct 1, a few members from the chapter visited the **Socare Ind**, an organization located at Laggere in Bangalore. Socare's mission is to make a difference in the lives of indigent children and make them contribute positively to society. It was amazing to see how the **society** is touching the needy and has been helping such deprived kids to live a life of entity, hope, and respect. Our chapter volunteers interacted and shared the basics of Information Security with children and donated certain sports kits to the children.

ISACA BC registered the updated bylaws' latest version in the ISACA HQ template after more than a decade and we thank all members who actively participated to complete this activity on time.

In pursuit of Digital Trust, ISACA is dedicated to advancing that trust to build a safer digital world for all. We will unlock a wide range of programs reserved for ISACA members in the coming months on Digital Trust. Our Chapter continues to engage members and provide value to members through online and in-person CPE sessions. Thank you all and our speakers for your active support and participation.

ISACA BC is planning to participate in Bengaluru TECH SUMMIT and intent has been shared with organizers. We will keep you posted on our participation.

Lastly and before I sign off, I would like to say a huge thank you to our chapter EC, members & sponsors for all the hard work for making 25th Annual Karnataka conference a fantastic and monumental event.

Our AGM is scheduled on 29th Oct 22 and requests all to attend the AGM and see you in AGM!

Regards,

RAJASEKHARAN K R, CISM, CDPSE®, CRISC®, PMP, ITIL (E), CSM, SAFe, ISO 27001 LA
Vice President

Message From Secretary

Warmest Greetings.

The pandemic has changed the world dramatically and has accelerated the development in the field of information technology. Enterprises are investing more in digital transformation such as cloud computing, Artificial Intelligence, blockchain as well as measures to improve their cybersecurity. With all these developments, auditing and/or management consulting in the field of information systems audit and control are becoming more crucial. We in ISACA and at Bangalore Chapter adapted to the new reality, more quickly and resourcefully than seemed possible at first.

Throughout this complicated process, our dedicated EC members remained steadfast committed to the Goals and our responsibilities to promote the education of and help expand the knowledge and skills of our members in the interrelated fields of auditing, quality assurance, security, IS audit and control, and IT governance. Our goal has been to keep everyone safe while still carrying on the important work of the Chapter and preserving it as a place of higher learning.

Much of this has required alternative delivery methods, with our CPE sessions being offered online. Though the pandemic precipitated this dramatic change, on the positive side we are learning a lot about what makes remote session effective.

We have overcome many setbacks in the past and will do so again. Our mission is clear, our values are strong, and our commitment to education and research is enduring. Yet I like to say that the world needs more from us.

We very much appreciate your continued commitment and hope to see you in our upcoming AGM 2022.

Regards,

VIJAYAVANITHA, CISA, CIA, MBA, M. Com,
Secretary

Renewal of ISACA membership for the year 2023

Warm Greetings from ISACA Bangalore Chapter!!!

We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

Visit www.isacabangalore.org for more information.

Now it is time for renewing your ISACA® membership for 2023 if not already done. Please ensure to renew your membership before the PURGE to ensure the benefits arising out of continued membership.

Please click below to renew *(login with your ISACA username and password to renew)*
http://www.isaca.org/renew

In case you need any assistance, please do not hesitate to reach out to Chapter Office at chapter@isacabangalore.org

For your information, the membership dues are indicated here below:

International Membership Dues: **$135.00**
ISACA Bangalore Chapter Dues: **$10.00**
Total Dues for 2023 membership renewal: **US$ 145.00**

Note: ***Apart from the above, certification maintenance dues may apply as per the certifications held.***

Recap of Chapter Programs in Q3, 2022

25th Annual Karnataka Conference held on 29th & 30th July 2022 at Sterlings Mac Hotels Pvt. Ltd., Old Airport Road, Bangalore.

SPEAKERS & PANELISTS

Dr. Aloknath De
Exec Consulting Director
Samsung India

Shane Cox
VP - Global Security
Optiv Inc.

Mr. Debashish Jyotiprakash
Vice President Asia
Qualys Inc

Vaibhav Koul
Managing Director
Cyber Security, Privacy and IT Governance
Protiviti Member Firm for India

Anand Prakash
Founder
PingSafe

Raghuraj Bandi
Founder & CEO
Call IN IT Solutions Pvt Ltd

Sovon Lal Mukherjee
CISO
Fincare Small Finance Bank

ANAND MURTHY RAJ
Director
Gladwell Academy

Mrudul Uchil
Senior Director & India Site Head
Tier Cybersecurity
VISA

Preeti Bhisikar
IBM

Suma. K
Vice President
Deutsche Bank

Kavitha Srinivasulu
Head Cyber Risk & Data Privacy- BFSI
TCS

SPEAKERS & PANELISTS

Kumar KV
Group CIO & CISO
Narayana Hrudayalaya Limited

Vaisakh T R
CEO
Prophaze Technologies

Lakshi Das
COO
Prophaze Technologies

Valan Sivasubramanian
Manager - Systems Engineering
Fortinet

Shashidhar CN
Founder and CEO of SecurIT
Consultancy Services

Mr Jayachandran
Director
eSecurityaudit

Pradeep Sekar
Director,
Cyber Strategy & Transformation,
Optiv

Alex Young
Director Engineering
Optiv Inc

Merril Cherian
Partner
KPMG India

A. Krupakaran
Board Member
INFHRA

Dr. Sandhya R. Anvekar
Program Head, Skilling, RITS,
Dept. of Electronics, IT, BT, Science & Technology
Govt of Karnataka

Vaidyanathan R Iyer(Vaidy)
Chief Of Operations
IBM Security Command Center
Asia Pacific

Satish Kumar Dwibhashi
Senior VP & CISO
InMobi Group

ISACA Bangalore Chapter

Annual Karnataka Conference

ISACA Bangalore Chapter

DAY 1

2022 - ISACA - BC - Annual Conference - Date - 29th July 2022

Time	
08:30 - 9:30	**Registration**
09:30 - 09:45	**Welcoming the Chief Guest & Keynote speaker to the venue**
09:45 - 09:55	Welcome by Conference Chair- ISACA BC Vice President **Mr. Rajasekharan KR**
09:55 - 10:00	**Chief Guest, Keynote speaker & ISACA office bearers ascend the dias** **Mr. Pratap Reddy** - Commissioner of Police, Bengaluru City Police, Government of Karnataka **Dr. Aloknath De** - Exec Consulting Director- Samsung India, Adjunct Prof–IISc, Bangalore
10:00 - 10:10	**Inauguration** - Lighting the lamp
10:10 - 10:20	**Welcome by ISACA BC - President** Mr. Velmuruga Venkatesh
10:20 - 10:40	**Inauguration address by Chief Guest** Mr. Pratap Reddy IPS (Commissioner of Police)
10:40 - 11:00	**"Cyber-Physical Systems and Digital Trust"** Dr. Aloknath De - Exec Consulting Director- Samsung India, Adjunct Prof–IISc, Bangalore
11:00 - 11:10	**Release the conference edition of newsletter by Chief Guest**
11:10 - 11:25	**Felicitation by Chief Guest (High exam scorers)**
11:25 - 11:45	**Exhibits & Tea Break**
11:45 - 12:25	**"Effective Detection & Response: Data Driven Decisions"** Mr. Shane Cox - VP Global Security Operations - Optiv Inc
12:25 - 13:05	**"Orchestration & Automation at scale: New ways of doing Vulnerability Management right"** Mr. Debashish Jyotiprakash - VP Asia- Qualys Inc
13:05 - 14:00	**Lunch Break**
14:00 - 14:30	**"Leading Organizations in a RUPT world"** Mr. M R Anand - Director - Gladwell Academy
14:30 - 15:00	**" Despite Best-in-Class Security Software and a great in-house team, why do Companies Still Run Bug Bounty Programs and Engage with White Hat Hackers?"** Mr. Anand Prakash - Founder PingSafe
15:00 - 15:30	**" Emerging cyber risk and mitigation strategies"** Mr. Vaibhav Koul - Managing Director – Cyber Security, Privacy and IT Governance, Protiviti Member Firm for India
15:30 - 15:45	**Exhibits & Tea Break**
15:45 - 16:35	**Women Panel Discussion** **Topic - Key Inflection Points - People, Technology, and evolving Security landscape** Ms. Suma. K - Vice President - Deutsche Bank (Moderator) Ms. Mrudul Uchil - Senior Director & India Site Head for Cybersecurity - VISA Ms. Kavitha Srinivasulu - Head Cybersecurity & Data Privacy - TCS Ms. Maj Preeti Bhisikar - IBM
16:40 - 17:15	**"Achieve your Data Security in your Digital Transformation Journey"** Mr. Sovon Lal Mukherjee - CISO - Fincare bank, Mr. Raghuraj Bandi - Founder & CEO at Call IN IT Solutions Pvt Ltd
17:15 – 17:25	Winners of Quiz
17:25 – 17:30	Vote of Thanks

ISACA Bangalore Chapter

Annual Karnataka Conference

ISACA Bangalore Chapter

DAY 2

2022 - ISACA - BC - Annual Conference - Date - 30th Jul

Time	
9:00 - 9.10	**Welcome by ISACA Bangalore Chapter - President**
9:10 - 9:40	**Chief Guest speech** - Mr. Sunil Panwar, IFS - Chief Executive Officer Center e-Governance, Government of Karnataka
9:40 - 10:00	**Keynote** Mr. Kumar KV - Group Chief Information Officer - Narayana Health
10:00 - 10:30	**" API security and zero-day attacks "** Mr.Vaisakh T R - CEO Prophaze Technologies and Ms Lakshmi Das - COO and product evangelist - Prophaze
10:35 -11:10	**"An Annual Perspective on Cyber Threat Predictions for 2022"** Mr. Valan Sivasubramanian - Manager - Systems Engineering - Fortinet
11:10 - 11:30	**Exhibits & Tea Break**
11:30 - 12:00	**"Don't fear the math - The value of low metrics"** Mr. Alex Young - Director Engineering – Optiv Inc
12:00 - 12:30	**"ILAIYARAAJA & art of Infosec"** Mr. C.N.Shashidhar - Founder and CEO - SecurIT Consultancy Services
12:30 - 13:00	**"The ethics of artificial intelligence: Issues and initiatives and Role of Auditor"** Mr. Jay Chandran - Director - eSecurity Audit
13:00 - 14:00	**Lunch Break**
14:00 - 14:15	**Quiz by ISACA BC ; Survey opportunities for Sponsors**
14.15 - 14:45	**"The hidden costs of insecure M&A transactions"** Mr. Pradeep Sekar - Director, Cyber Strategy & Transformation – Optiv Inc
14:45 - 15:15	**" The Impact of Artificial Intelligence on Cyber-Resilience"** Mr. Merril Cherian - KPMG - Partner
15:15 - 15:30	**Exhibits & Tea Break**
15:30 - 16:20	**Panel Discussion** **Topic - Can Super Human & AI Cybersecurity Defence can stop Ransomware Strike?** Mr. Vaidyanathan Iyer, COO IBM Cybersecurity Command Center (Moderator) Mr.Alex Young - Director Engineering - Optiv Inc Mr. Debashish Jyotiprakash - VP Asia- Qualys Inc Mr. Satish Kumar Dwibhashi - Senior Vice-President & CISO - InMobi Group
16:25 - 16:55	**"Better be circumspect, when in doubt to secure your life"** Mr. A.Krupakaran - Board Member - INFHRA
17:00 - 17:10	**Facilitations / Winners of Quiz; Social Media**
17:10 - 17:20	**Valedictory Address** Dr Sandhya R. Anvekar, Program Head: Skilling, KITS, Dept. of Electronics, IT, BT, Government of Karnataka
17:20 - 17:30	**Vote of Thanks** Ms. Vijaya Vanitha ISACA Bangalore Chapter - Secretary

1. **Topic : "Quantum Computing - An Introduction, Brief History & Future Direction"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 20-Aug-2022 (Saturday) Time : 5:00 PM - 7:00 PM IST
   2 CPE Credits offered

The session covered:

- Quantum Computing & Brief History
- Security Implications of Quantum Computing
- Quantum Computing – Business Applications
- Quantum Security – Business Use Cases
- Quantum Security Use Cases
- Quantum Cryptography – Tech Stack
- Quantum Computing – Latest Developments & Indian position

Speaker Profile: Aseem Rastogi

Aseem, Head of CyberSecurity @Meesho is an Information Security professional with 24 years of experience. His expertise is in scaling security 0 to 1, setting up high performance CyberSecurity teams and deliver 10x process driven outcomes. Prior to Meesho, he was headed CyberSecurity function at Razorpay.

He also had an entrepreneurial stint where he built, a CSPM product CloudOptics, back in 2017

2. **Topic : "APT Attacks and Content Disarm & Reconstruction"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 10-Sep-2022 (Saturday) Time : 5:30 PM - 6:30 PM IST
   1 CPE Credit offered

Last three years, most APT attacks have happened using pdf, doc and image files infected by 0day exploit.

The session covered the following:

- APT attacks

- What are CDR technologies and how to use them to reduce risk to an organisation

- Stegano Malware and exploits

Speaker Profile: Suriya Prakash

Mr Surya is the Head – DARWIS SFS & Threat Intel API of CySecurity Corp, US. He is founder shareholder & director of CySecurity Pte Ltd. He is in the Hall of Fame of Google, Facebook. He has found critical vulnerability in both the organization. He has extensive knowledge on blockchain and has found major vulnerability on multiple blockchains.

3. Topic : "Targeted Ransomware"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 24-Sep-2022 (Sunday) Time : 5:30 PM - 7:30 PM IST
2 CPE Credit offered

For consecutive years now, ransomware remains one of the top risks and an attractive business model for cyber criminals.

The session covered:

1. Understanding ransomware - How it works (live demo)
2. Understanding the ransomware economy
3. Current statistics and trends on ransomware
4. Top three ransomware attacks and lessons learned
5. Incident response for ransomware
6. Cyber insurance and ransomware
7. Playbooks/Runbooks
8. Negotiating with attackers
9. Recovering from ransomware attacks
10. Dark web monitoring (live demo)

Speakers Profile: Aniket Amdekar and Tulika Ghosh

Mr Aniket S Amdekar, General Manager - Cyber Defence Education, Great Learning

Specialization in E-Commerce security (End to End). Liaise with internal and external teams to ensure security best practices are defined and implemented across MakeMyTrip's product line. Research, design and implement cutting-edge security technology/processes that would help keep up with ongoing threats.

Ms. Tulika Ghosh, Vice President, Morgan Stanley

Certified Information Security professional with over 15 years of experience in leading and delivering Information security, cyber strategy, and transformation programs for global corporations. She also has extensive experience in helping organizations with their regulatory and privacy compliance posture

4. Topic : "ISACA Community Day"
Date : 01-Oct-2022 (Saturday) Time : 3:00 PM - 5:00 PM IST

ISACA Community Day was celebrated on 1st October 2022 at SocareInd - Society's Care for Indigent, an NGO located in Bangalore. SOCARE's mission is to make a difference in the lives of indigent children and make them contribute positively to the society. President of ISACA Bangalore Chapter Mr. Venkatesh interacted with the children and conveyed to them the objectives of the ISACA community day. Director membership Mr.Ramachandra Upadhya spoke about importance of cyber security and gave the basics of cyber security to the children. All the volunteers also individually interacted with the children.

We distributed few sports Kits to the children which brought lot of excitement to the Children.

5. ISACA Bangalore Chapter - Notice for Special General Body Meeting on 15th October 2022
Venue : Pride Hotel, 93, Richmond Road, Langford Gardens, Bengaluru - 560 025.
Date : 15-Oct-2022 (Saturday) Time : 11:30 AM - 1:00 PM

SPECIAL BUSINESS:

To consider and if thought fit, to pass with or without modification(s) the following as an Ordinary Resolution:

Procurement of New Office Building for ISACA Bangalore Chapter

ISACA Supported Events :

1. 5-day Online ISO 27001:2013 based Lead Auditor Training Course organized by ISC Global FZ LCC & CPG Assurance Pvt. Ltd., Mumbai from 18-Jul-2022 to 22-Jul-2022

ISC Global Accredited Instructor - Mr. Ganesh / Mr. Ketan Shah

ISACA Members earned credit of 35 CPE hours in accordance with ISACA Guidelines. They got substantial discount in registration fees.

2. TFCI Events Private Ltd & Data Privacy Policy India Tech & Law Conclave 2022 on 21-Sep-2022.

Cloud Computing Challenges and Benefits in this Digital Era

- Kavitha Srinivasulu C
Global Head of Cyber Risk & Data Privacy - BFSI R&C, TCS

About the Author:

Kavitha is an experienced professional in Cyber Security, Risk Management, Vendor Technology Management, Enterprise Risk Management, BCMS, ISMS,GDPR, Data Privacy, Compliance & Program Management, End to end deliverables and Information Protection, with a career spanning around 16+ years on financial services and telecom domains.

As the world is changing from old traditional infrastructures to becoming more cloud-based and focusing on data protection in this digital era is explicit. Cloud adoption has increased significantly during the COVID phase as connecting from anywhere became a new normalcy of work. Based on the availability, scalability, and flexibility of cloud computing, most of the organizations have shifted from old legacy models to software as a service to work in a undisrupted environment with full access.

There are many sources of risks and challenges prevailing in the current threat landscape while adopting to cloud, however, every organization needs a very affordable, scalable, flexible, and fast methodology to speed up the services for their consumers. Cloud security helps the cloud computing model with various kinds of security controls such as data availability, data storage, computing resources, servers, applications, some networks capability, developing tools, open access, flexibility etc. These controls are built and managed by engaging with Cloud Service Providers (CSP) using a shared responsibility model to increase resilience and data protection.

Organizations are moving more and more of their data and applications to the cloud day by day. A recent report forecasted that, by 2025, 80% of enterprise workloads will be in the cloud. Emerging cloud computing technologies have created numerous risks and challenges while building an innovative technology for business growth. Some of them like -

Cloud Adoption Challenges:

These emerging risks isn't startling as the benefits that the cloud services are providing from scalability, accessibility with cost reductions is beneficial to business. An organization can avoid several issues that affects the operations of the company by using the cloud platform solutions.

Cloud security challenges increase day by day due to massive volumes of data stored, managed, and processed through a network of shared services reducing the cost of IT infrastructure. When it comes to implementing a cloud-based solution, many organizations are concerned about data security, data loss and cyber-attacks. Let's look at some of the security measures enabling which can protect the data in cloud computing and witness in the future of complete cloud migration.

1) Serverless Computing

Serverless computing is a cloud approach in which the customer doesn't have to deal with infrastructure administration and server provisioning. Instead, the cloud service providers manage the supporting infrastructure and distribute computing power following the demand. In this cloud computing approach, there is an enormous amount of Risk and compliance attention required to ensure the governance of the cloud computing model is designed and data is protected.

2) Authorized controls

Administrators can manage access from anywhere on a cloud-based access control system, even from a phone at home, rather than from a single computer in the office. That's especially important during a time when many people are working from home due to COVID-19.

Access controls play a key role in enabling right level and privileged access in the cloud environment to avoid unauthorized accesses ending up in data thefts. Access controls are designed effectively to revoke instantly from a browser or phone, and the process can be automated via Single Sign On integrations. Companies using the traditional model experience frequent access leaks/data loss from insider threats.

3) Business Continuity (BCP) / Disaster Recovery (DR)

A business can use cloud business continuity and disaster recovery framework to create recovery strategies aligning to business requirements, back up data and create a standby IT environment that can take over if the primary infrastructure fails / business disruptions

4) Increased Uptime

Operations/Delivery downtime due to business interruptions and data loss can cause a huge impact to business. With implementing business continuity in cloud, we can continuously monitor, evaluate, and automatically replicate data minimizing the downtime during a disruption.

5) Secure Access Service Edge (SASE)

SASE allows users to stably manage and regulate access across end-user devices, on-premises IT, and cloud apps.

6) Data Protection

Data protection in the cloud can be a challenging endeavor, especially when it comes to distributed and complex infrastructures like Public Cloud, Multicloud and hybrid clouds. If we are using more than one cloud vendor or multiple cloud services, we're going to need to work harder to secure the data in the risk prone threat landscape. Proactively identify and mitigate risks, such as security threats, suspicious user behavior, malware and others in applications and other sources for data protection.

7) Continuous compliance validation

Different laws and regulations are sticking to the adoption of cloud infrastructure. As a result, regular compliance reviews and audits are essential to adhere to the legal and regulatory requirements. There are huge expectations from regulators side which differs from geo to geo on the standards to comply with. Performing cloud security assessments and creating a threat free environment by continuous monitoring is the key to reduce business risks.

Users worldwide access an open pool of resources, including apps, services, servers, data, and computer networks to continue their day-to-day activities in the new work environment of WFH. Cloud computing helps to manage public, private or hybrid model to make it possible. It improves data access and eliminates inconsistency in subsequent updates. Cloud security services build a skeleton of securing the data managed in cloud through Access controls, Data Protection, Business Continuity, Boundaryless Governance, Incident Management, and modernization to effectively control the data at rest and data in transit.

As a result of adopting to cloud services, we avoid the upfront infrastructure cost, single ownership, data protection and in maintaining complex IT infrastructure. Some of the cloud security benefits are:

Cloud Security Benefits:

Most on-premises systems require downtime and lots of complex software upgrades patches that takes lot of time and manpower. These typically must be done in regular intervals to avoid any security risks. Cloud-based systems play a key role in automatically backing up and replicating the data without requiring any intervention from the business. Cloud computing network is a fast-growing network-based technology without leaving exceptions for vulnerabilities or risks. It's very essential for building the cloud computing model with appropriate security controls to ensure security ambience and business resilience.

Content Disarm and Reconstruction

- J Prasanna
Founder & Director - CySecurity Corp & Cytech Ventures LLC

About the Author:

PRASANNA is a serial entrepreneur and currently is the Founder & Director of CySecurity Corp & Cytech Ventures LCC.

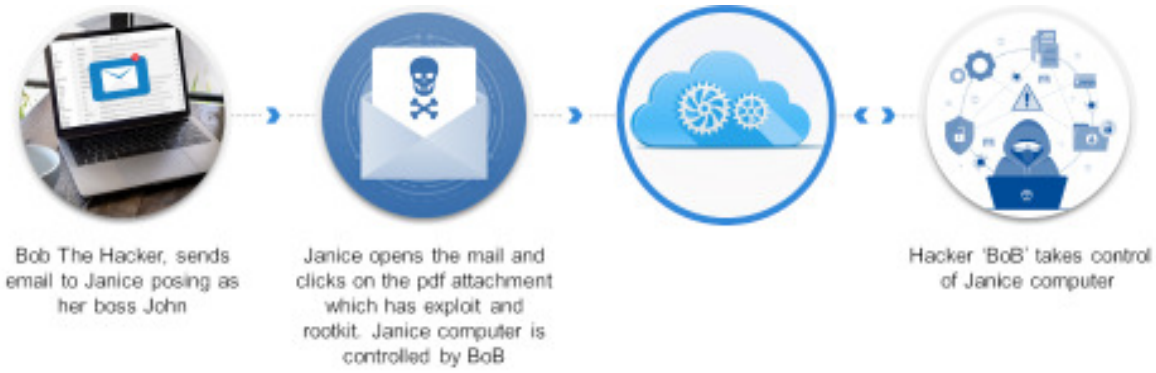
This whitepaper describes the importance of Content Disarm and Reconstruction and gives a quick glimpse of the CDR technology. The objective of this paper is to provide insight on how weaponization of PDFs/doc/docx is a new threat that security experts work tirelessly to identify, research, and develop new ways to guard, using the CDR technology.

Market Trends & Challenges

Cybercriminals find creative new ways of misdirection and obfuscation. Hackers have recently been using PDF/DOC/DOCX/IMAGE files in new and very lethal ways. Additionally, Ransomware groups have been responsible for infecting hundreds of servers with malware to gain corporate data or digital damage systems, essentially spreading misery to individuals and hospitals, businesses, government agencies and more all over the world. Weaponization of PDF/DOC/DOCX is one such new threat.

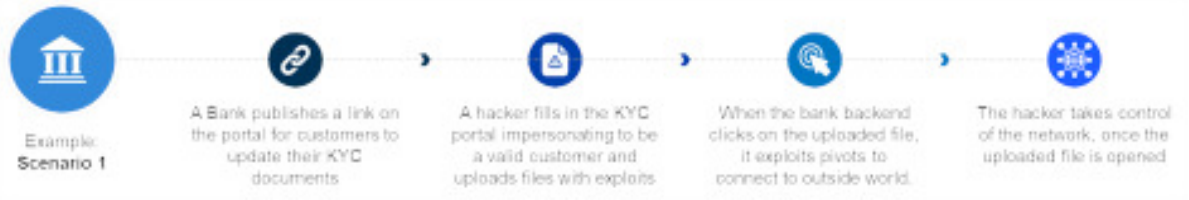
Sharing below some examples of how exploits are being implemented by hackers:

PDF/DOC exploits:



The above example shows how Janice opens an email from a hacker who poses himself as her boss. Janice assumes the mail to be from her boss and clicks on the PDF attachment which has an exploit. The moment Janice clicked on the attachment in the mail, the hacker took control of Janice's computer through cloud. This is a highly likely scenario in any organisation/industry.

File Upload



In the above-mentioned scenario, with KYC being the prime requirement in any bank, when a Bank publishes a link on their portal for customers to update their KYC documents, a hacker, impersonating to be a valid customer fills the KYC form and uploads files with exploits. The hacker takes control once the Bank, assuming the user to be a valid customer clicks on the uploaded file.

In the above scenario, an APT attack hacker, in order to get access to various departments of an organization, will upload exploit DOC/PDF. For example, the hacker might upload resume to HR portal, a contract to the Legal department in the guise of a contractor, an invoice to the finance department as a vendor. When any of these departments' representatives click on the infected attachment, the malware immediately connects back to the hacker. The hacker get access to the organization network.

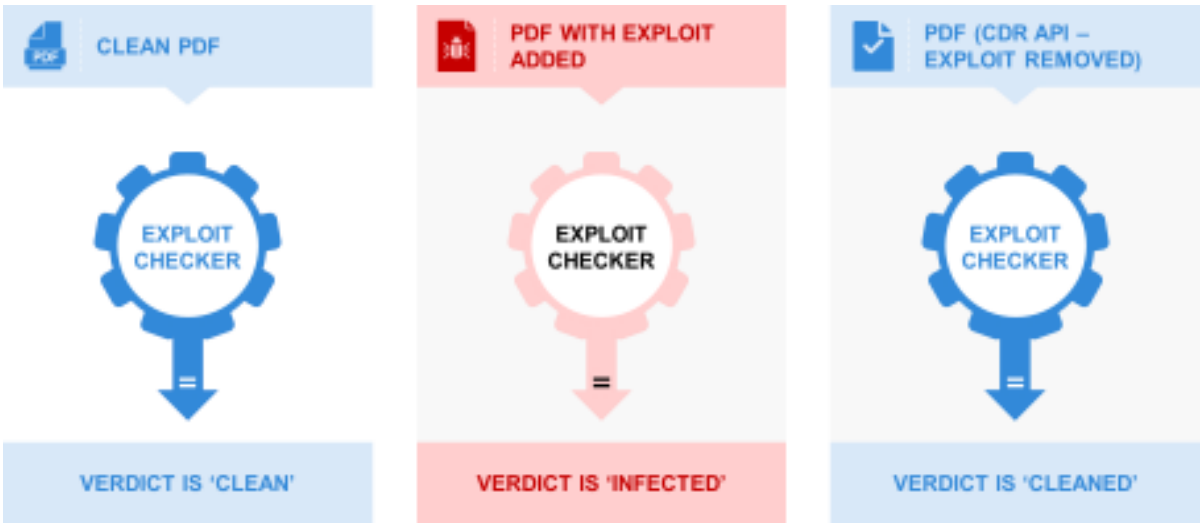
Content Disarm and Reconstruction (CDR) – The Solution

To help organisations from situations mentioned above, CDR (Content Disarm and Reconstruction) also known as Threat Extraction, proactively protects against known and unknown threats contained in documents/image/pdf by removing malware,exploits. The WS7 API is written using the CDR method. WS7PDF is primarily for pdf file. In the process of checking for malicious files/exploits, the pdf document is disarmed and reconstructed. This enables CDR to offer true zero-day prevention, while delivering files to users/customers quickly.

WS7IMG is primarily for image files with image extensions such as TIFF, JPG, PNG, GIF, BMP etc. A unique technology is used to disable the malicious stegano malware which could be hidden inside the image. The disarmed image is optionally given as a JPG file.

Shown below are two examples for easy understanding:

Example 1: PDF Exploit



In the above example, there are 3 scenarios that display what the verdict of the exploit checker is when a clean PDF is passed, when a PDF with exploit added is passed and the verdict when the PDF goes through the CDR API. In the first scenario above, the verdict shows as 'CLEAN' for a PDF with no exploit. Similarly, when an exploit was added to a PDF, the verdict shows as 'INFECTED' by the exploit checker. Finally, when the PDF file is run through CDR engine, the exploit is removed and verdict shows as 'CLEANED'.

The below screenshots show the backend query that the CDR engine runs for different scenarios.

1) When we analyse a clean file (fig 1 - original.pdf), the output shows as 'Nothing detected':

Fig: 1

```
uocx@uocx-TE:~/Desktop/DEMO$ ./check.sh original.pdf
{
    elapsed: 4.188247919082642,
    execute: 0,
    exploit: 0,
    feature: 0,
    filename: original.pdf,
    finished: 1662528027.9289052,
    header: 255844462d312e338a25c4e5f2e5eba7,
    md5: b8f32750d8962c60fd9089bd0537d897,
    packages: [],
    exe.yara: 1662288787.9080794,
    exploits.yara: 1662288787.9080794,
    pdf.yara: 1662288787.9080794,
    rating: 0,
    results: {},
    risk: nothing detected,
```

2) We analyse evil.pdf (fig 2), and when an exploit is detected, the exploit checker shows the number of malicious content present (Fig 3) and gives a comment as 'high risk active content' (Fig 4):

Fig: 2

```
uocx@uocx-TE:~/Desktop/DEMO$ ls -a
.  ..  check.sh  evil.pdf  original.pdf
```

Fig 3

```
uocx@uocx-TE:~/Desktop/DEMO$ ./check.sh evil.pdf
{
    elapsed: 4.201820373535156,
    execute: 8,
    exploit: 0,
    feature: 2,
    filename: evil.pdf,
    finished: 1662528218.1774423,
    header: 25504446?d312e330a25c4e5f2e5eba7,
    md5: aea2b46ec2fc226672c3f3bf8cd92495,
    packages: [],
    exe.yara: 1662288787.9888794,
    exploits.yara: 1662288787.9080794,
    df.yara: 1662288787.9888794,
    rating: 2,
    results: {
        root: [
            {
                desc: suspicious.javascript object,
                mitre: T1827 T1859.887,
                rule: suspicious_javascript_object,
                type: pdf
            },
            {
                desc: suspicious.pdf embedded PDF file,
                mitre: T1204.882,
                rule: suspicious_pdf_embedded_PDF_file,
                type: pdf
            },
            {
                desc: pdf.exploit execute EXE file,
                mitre: T1203 T1204.882,
                rule: pdf_exploit_execute_EXE_file,
                type: pdf
            },
            {
                desc: pdf.warning OpenAction,
                mitre: T1203 T1204.882,
                rule: pdf_warning_openaction,
                type: pdf
            },
            {
                desc: pdf.exploit access system32 directory,
                mitre: T1203 T1204.882,
                rule: pdf_exploit_access_system32_directory,
                type: pdf
            },
            {
                desc: pdf.exploit execute action command,
                mitre: T1203 T1204.882,
                rule: pdf_exploit_execute_action_command,
                type: pdf
            },
            {
                desc: pdf.execute access system32 directory,
                mitre: T1203 T1204.882,
                rule: pdf_execute_access_system32_directory,
                type: pdf
```

Fig 4

3) When Exploit Checker runs the CDR engine (Fig 5), removes malicious content, disassembles the file (fig 6) and shares a clean pdf as an output. Fig 7 shows the final result as clean pdf with no exploits detected:

Fig 5

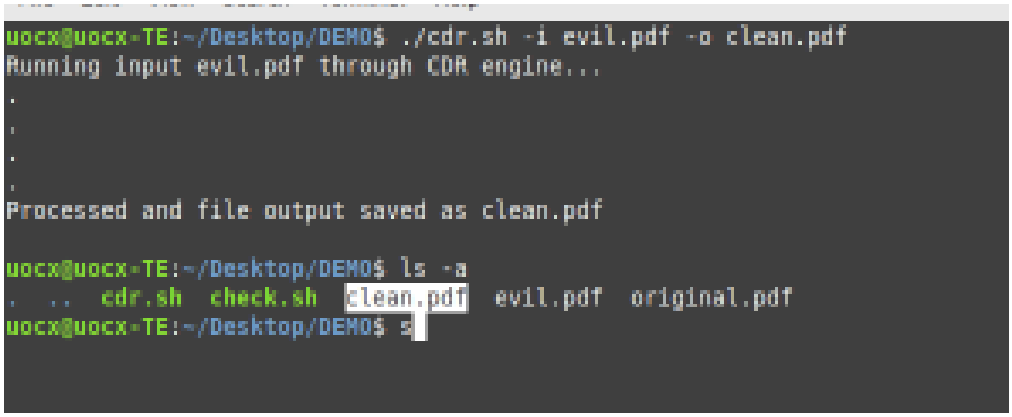


Fig 6

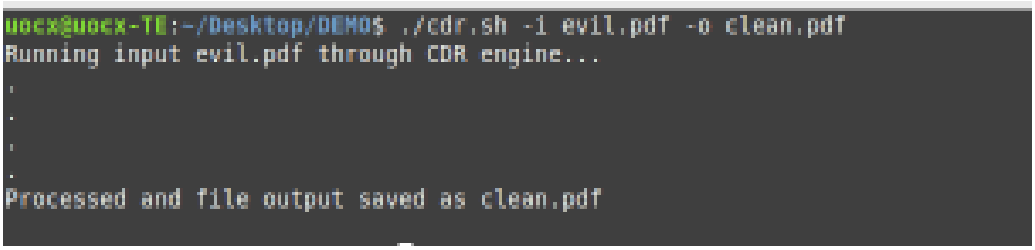


Fig 7

```
uocx@uocx-TE:~/Desktop/DEMO$ ./check.sh clean.pdf
{
    elapsed: 3.5926151275634766,
    execute: 0,
    exploit: 0,
    feature: 0,
    filename: clean.pdf,
    finished: 1662528697.6275551,
    header: 255844462d312e378a25c7ec8fa28a25,
    md5: d73d241d52cbed87b23200308f5f5bbc,
    packages: [],
    exe.yara: 1662288787.9080794,
    exploits.yara: 1662288787.9080794,
    pdf.yara: 1662288787.9080794,
    rating: 0,
    results: {},
    risk: nothing detected,
    score: 0,
```

4) Comparison of Clean file Vs File with Exploits

Please note, the below screenshot shows the original pdf on the left side and the file with exploits (evil.pdf) on the right side. On the original pdf, there is no scroll bar as the file is only that long as visible. However, on the evil.pdf, with exploits in the file, the scroll for the entire file is longer than the original.

Fig 8

When we analyze evil.pdf (fig 9), shows the below message

Fig 9

```
uocx@uocx-TE:~/Desktop/DEMO/PDFCOMPARE$ ls -a
.  ..  evil.pdf  original.pdf
```

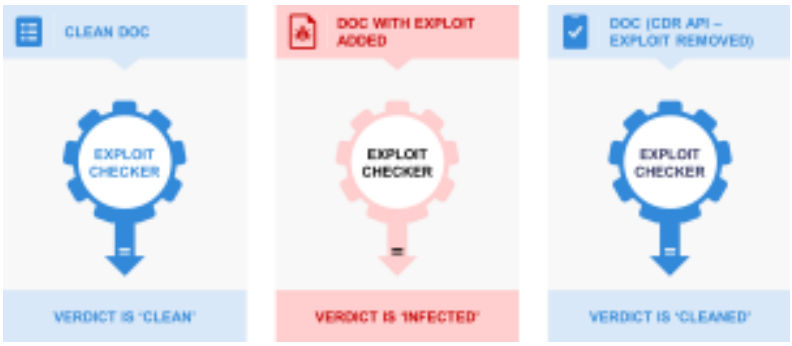
The image on the right side highlighted in red shows the embedded content with exploits in a binary data format (fig 10 & 11)

Fig 10

Fig 11

Example 1 and 2 shows how the CDR engine works to disassemble the file and reconstructs a clean pdf without exploits

Example2: DOC/DOCX Exploit

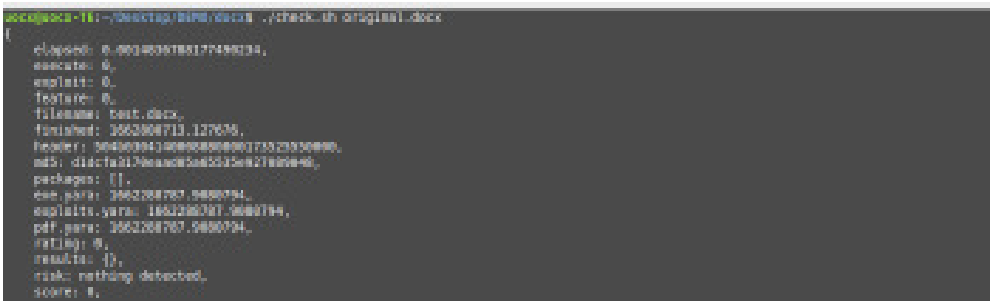


Similar to the previous example, in the current one, there are 3 scenarios that display what the verdict of the exploit checker is when a clean DOC/DOCX file is passed through the exploit checker. In the first scenario above, the verdict shows as 'CLEAN' for a DOC file with no exploit. Likewise, when an exploit was added to a DOC, the verdict shows as 'INFECTED' by the exploit checker. Finally, when the DOC file is run through CDR, the exploit is removed and verdict shows as 'CLEANED' by the exploit checker.

The below screenshots show the backend query that the CDR engine runs for different scenarios for a DOC file:

1) When we analyze a clean file (fig 12 – original.docx), the output shows as 'Nothing detected':

Fig 12



2) We analyze evil.docx (fig 13). When an exploit is detected in a doc file, the exploit checker displays the number of malicious content present with the risk comment showing as 'high risk active content' (fig 14):

Fig 13

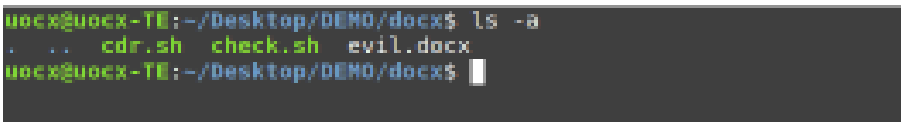
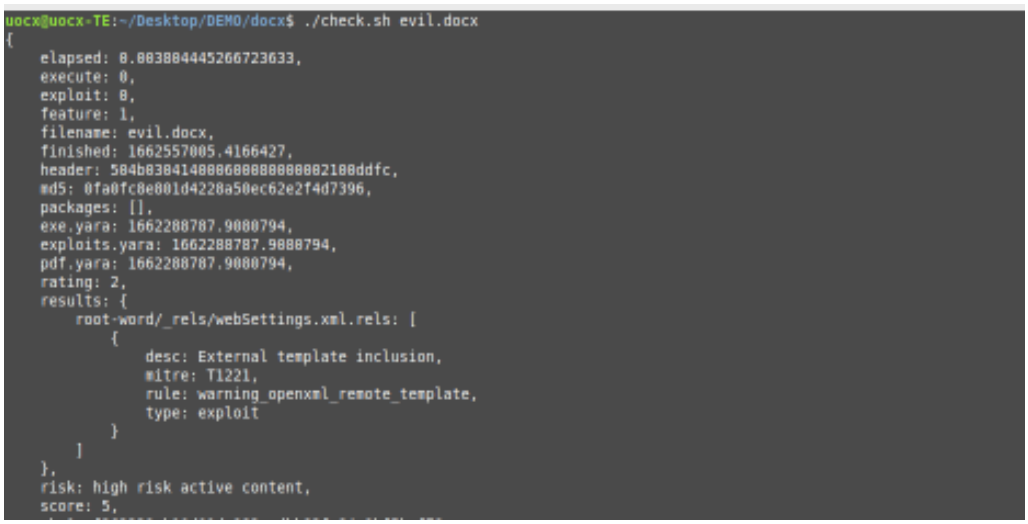


Fig 14



3) When an infected file is run through the CDR engine (fig 15), the file is disassembled and a clean PDF is created as an output (fig 16). The final output shows that there is 'nothing detected' with a score of 0 (fig 17)

Fig 15

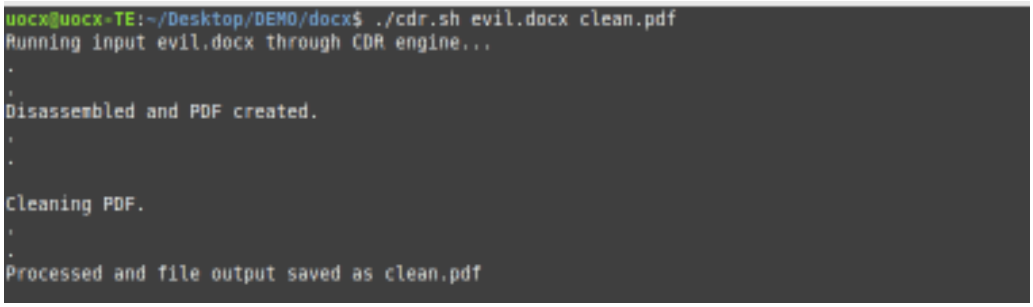


Fig 16

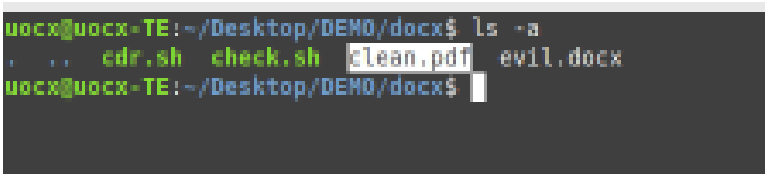
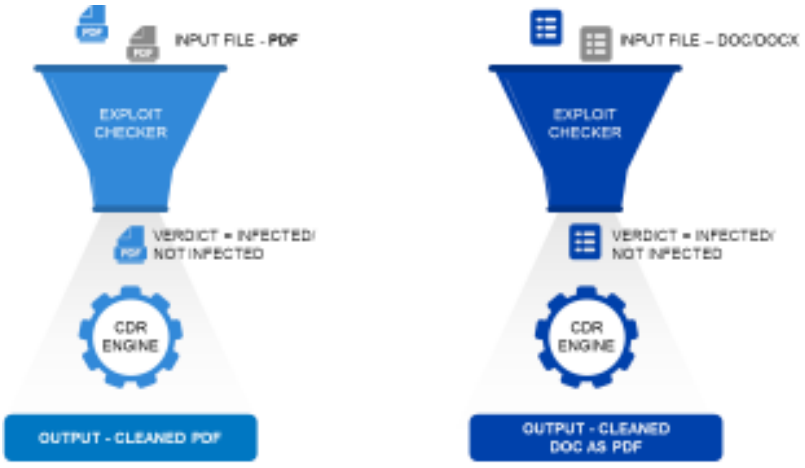


Fig 17

```
uocx@uocx-TE:~/Desktop/DEMO/docx$ ./check.sh clean.pdf
{
    elapsed: 0.002408851547241211,
    execute: 0,
    exploit: 0,
    feature: 0,
    filename: clean.pdf,
    finished: 1662557391.868889,
    header: 255044462d312e370a25c7ec0fa20a25,
    md5: aee5b927e3bc9cfa13e3d11e5d4886f6,
    packages: [],
    exe.yara: 1662288787.9888794,
    exploits.yara: 1662288787.9888794,
    pdf.yara: 1662288787.9888794,
    rating: 0,
    results: {},
    risk: nothing detected,
    score: 0,
```

CDR API – The Technology

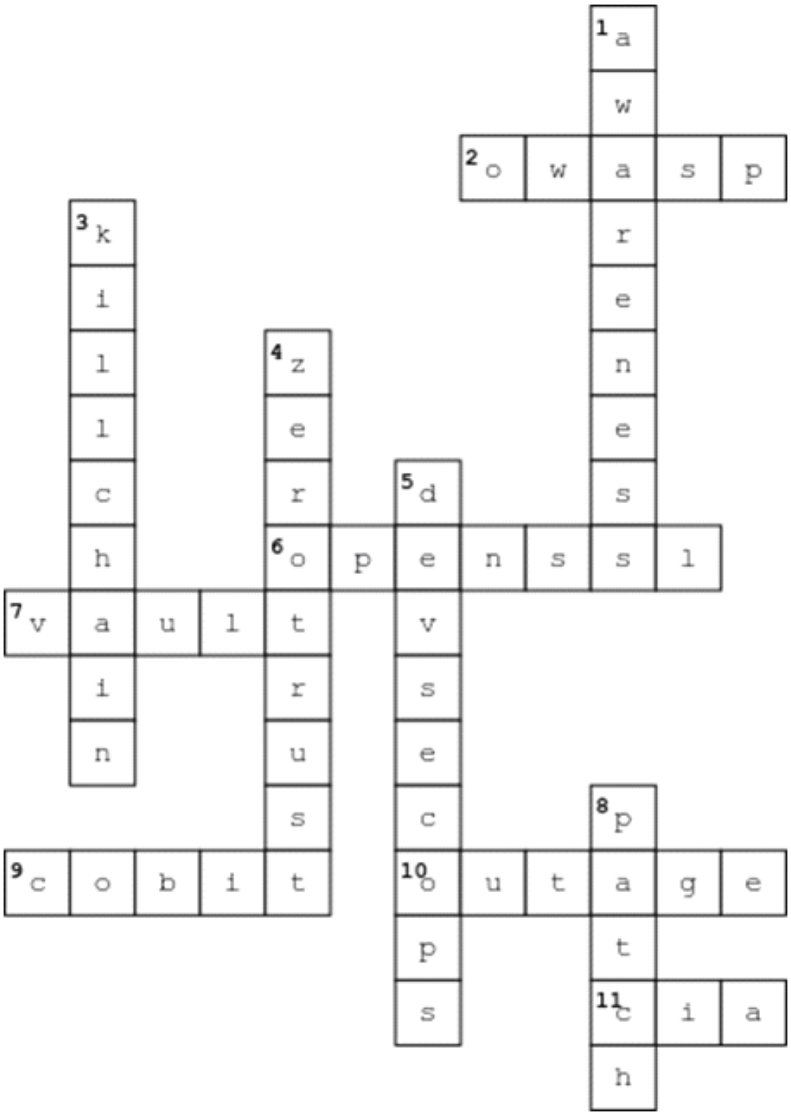


To summarize, when a customer subscribes to CDR API, any attachment that comes from external source in the form of PDF/DOC/DOCX file, the exploit checker processes the input file (PDF/DOC/DOCX) through the CDR engine and shares a cleaned file (PDF/DOC/DOCX) as an output.

Conclusion

The next time someone sends you an email with a PDF/doc/docx attachment, with the CDR subscription, one need not worry before clicking to open the file. CDR ensures to remove the exploits, disarm the file and reconstruct a clean file. This solution is highly recommended for all web applications, mobile applications and O365.

Answers for Q2, 2022 Crossword



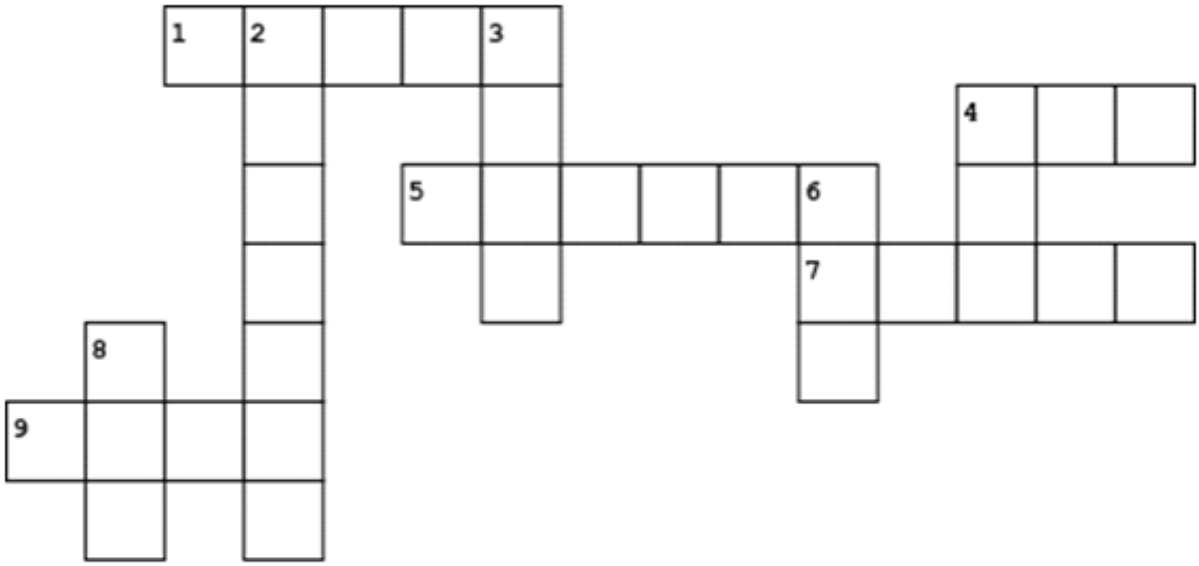
Winners of Q2-2022 Crossword Context:

1. Anshu Chaudhary - Membership ID: 1271400
2. George Joseph - Membership ID: 231586
3. Raghav Rachuri - Membership ID: 144201

Congratulations to the winners…!!

Each winner will get a gift voucher worth of Rs.500 each. ISACA Bangalore Chapter team will contact the winners.

ISACA BANGALORE CHAPTER CROSSWORD CONTEST - Q3, 2022



Across	Down
1. way to create a secure software **4.** is a security as a service offering designed to offer an alternative to an in-house Security Operations Center (SOC) **5.** a computer malware program that was originally developed in the form of a banking Trojan **7.** integrates all of the cloud security capabilities into a single cloud-native solution **9.** Toughest privacy and security law in the world	**2.** malicious software designed to enter your computer device, gather data about you, and forward it to a third-party without your consent **3.** to create a means for security solutions from different vendors to work together effectively to achieve certain security goals. **4.** method that requires the user to provide two or more verification factors to gain access to a resource **6.** is an estimation of the expenses associated with purchasing, deploying, using and retiring a product or piece of equipment **8.** is a new approach to threat detection and response that provides holistic protection against cyberattacks, unauthorized access and misuse

Crossword Created by Ganesan Ramani, Director - Newsletter, ISACA Bangalore Chapter

Three lucky winners will be awarded Rs.500 gift voucher each.

All the responses will be sent to chapter manager email address (chapter@isacabangalore.org).The responses should contain the photo / scanned copy of the filled crossword, Member name, ISACA ID, email and contact phone number.

Last date for sending the crossword results is November 25th, 2022.

Terms & Conditions:

a. This contest is only for ISACA Bangalore Chapter members only. Other ISACA chapter members and non-members are not eligible to participate in the contest.
b. In case if there are only one or two winners from the total entries then the vouchers will be given only to them. If there are no winners then no gift vouchers will be given.
c. ISACA Bangalore Chapter Executive committee reserves all rights to drop / change this program, modify the gift vouchers value

Contributions to ISACA Bangalore Chapter Newsletter

Dear Members,

The ISACA Bangalore Chapter Quarterly Newsletter covers the updates on chapter events, technical articles and whitepapers related to the areas of emerging technologies, IT Governance, Audits and Cybersecurity. In this regard, we encourage our chapter members to send your technical articles and whitepapers to us.

You can send your articles / whitepapers to our chapter email address: chapter@isacabangalore.org

Regards,

Ganesan Ramani
Director - Newsletter, ISACA Bangalore Chapter

Support from ISACA Bangalore Chapter

Website: https://engage.isaca.org/bangalorechapter/home

Chapter Office Address:
S/13, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.

T: 8050030042 / 98865 08515 / 080-23377956

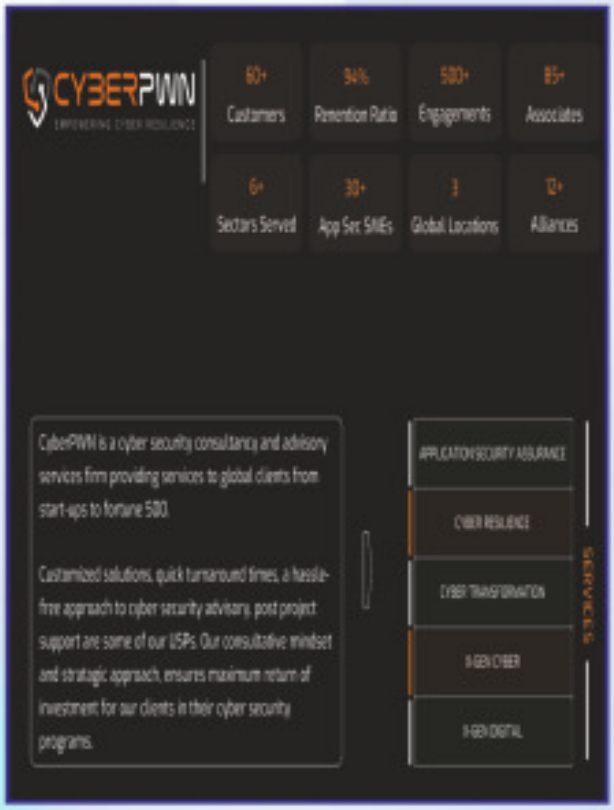
Email: chapter@isacabangalore.org

Telegram Channel: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA

LinkedIN: https://www.linkedin.com/company/isacabc/

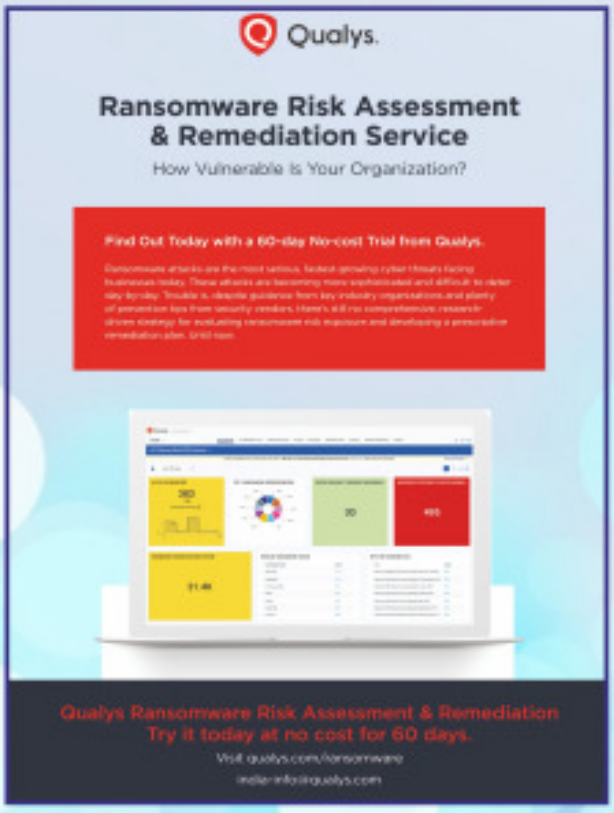
YouTube: https://www.youtube.com/channel/UCTdsKxe3t3BDCVGNrcUFhjg

Facebook: https://www.facebook.com/ISACABC/3


CYBERPWN
EMPOWERING CYBER RESILIENCE
60+
Customers
94%
Retention Ratio
500+
Engagements
85+
Associates
6+
Sectors Served
30+
App Sec SMEs
3
Global Locations
12+
Alliances
CyberPWN is a cyber security consultancy and advisory services firm providing services to global clients from start-ups to fortune 500.
Customized solutions, quick turnaround times, a hassle-free approach to cyber security advisory, post project support are some of our USPs. Our consultative mindset and strategic approach, ensures maximum return of investment for our clients in their cyber security programs.
APPLICATION SECURITY ASSURANCE
CYBER RESILIENCE
CYBER TRANSFORMATION
X-GEN CYBER
X-GEN DIGITAL
SERVICES


protiviti
Global Business Consulting
EMBRACING OPPORTUNITIES
THROUGH EMERGING TECHNOLOGIES
We help companies make the promise of digital transformation a reality.
Internal Audit
Business Operations Improvement
Strategy & Transformation
Data Analytics
Governance, Risk & Compliance
Human Capital Consulting
Technology Consulting
Forensic Services
Transaction Services
Cyber Security Services
Financial Risk Management
Digital Transformation
Our India offices:
Bengaluru
Phone: +91.80.6780.9300
Delhi NCR
Phone: +91.124.661.8600
Kolkata
Phone: +91.33.6657.1501
Chennai
Phone: +91.44.6131.5151
Hyderabad
Phone: +91.40.6658.8700
Mumbai
Phone: +91.22.6626.3333
India@protivitiglobal.in
www.protiviti.in


Prophaze
The New Phase of Security
WAF 3.0
The New Phase of Security
Application Security
API Security
Bot Protection
DDoS Mitigation


Qualys.
Ransomware Risk Assessment & Remediation Service
How Vulnerable Is Your Organization?
Find Out Today with a 60-day No-cost Trial from Qualys.
Qualys Ransomware Risk Assessment & Remediation
Try it today at no cost for 60 days.
Visit qualys.com/ransomware
india-info@qualys.com

Book Post

If undelivered please return to :

ISACA
Bangalore Chapter
S-13, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.
Ph. : 080-23377956 Email: chapter@isacabangalore.org

Printed @ Courtesy Ent. © 22128202

Chapter Reg No : 433/2002-2003