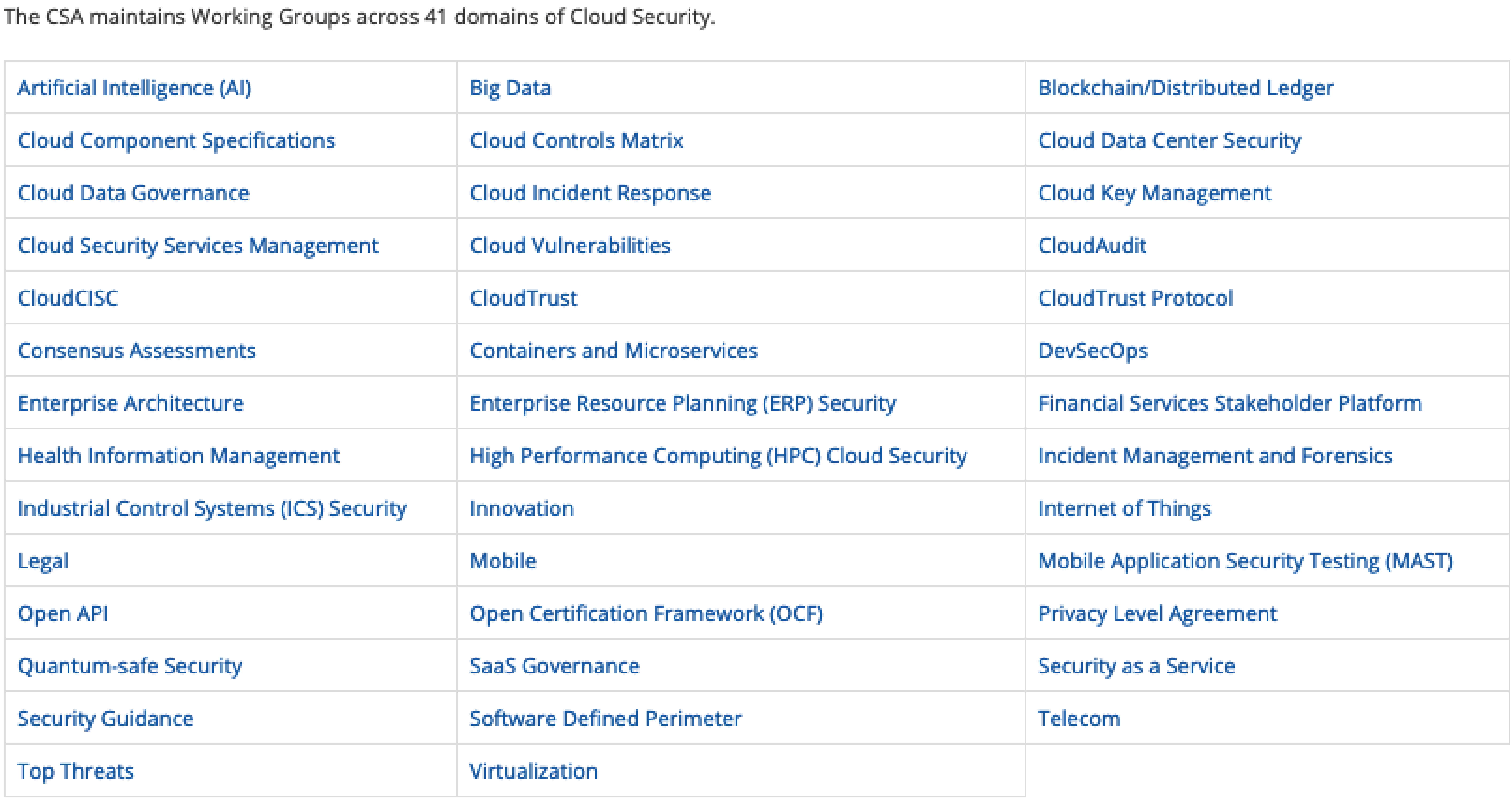
INTRODUCTION TO HPC CLOUD SECURITY WORKING GROUP

Ong Guan Sin
Co-Chair, HPC Cloud Security WG
Head, New Services & Cybersecurity,
National Supercomputing Centre

Zhuang Haojie
Research Director, APAC
Cloud Security Alliance

CSA cloud security alliance®

Like to Join one of CSA's Working Groups?



The CSA maintains Working Groups across 41 domains of Cloud Security.

Artificial Intelligence (AI)	Big Data	Blockchain/Distributed Ledger
Cloud Component Specifications	Cloud Controls Matrix	Cloud Data Center Security
Cloud Data Governance	Cloud Incident Response	Cloud Key Management
Cloud Security Services Management	Cloud Vulnerabilities	CloudAudit
CloudCISC	CloudTrust	CloudTrust Protocol
Consensus Assessments	Containers and Microservices	DevSecOps
Enterprise Architecture	Enterprise Resource Planning (ERP) Security	Financial Services Stakeholder Platform
Health Information Management	High Performance Computing (HPC) Cloud Security	Incident Management and Forensics
Industrial Control Systems (ICS) Security	Innovation	Internet of Things
Legal	Mobile	Mobile Application Security Testing (MAST)
Open API	Open Certification Framework (OCF)	Privacy Level Agreement
Quantum-safe Security	SaaS Governance	Security as a Service
Security Guidance	Software Defined Perimeter	Telecom
Top Threats	Virtualization	

Visit: https://cloudsecurityalliance.org/research

CSA APAC Research Initiatives

Working Groups (WGs)

- Cloud Incident Response
- Cloud Component Specifications
- Cloud Security Services Management
- Cloud Controls Matrix – ABS Cloud Computing Implementation Guide Mapping
- High Performance Computing (HPC) Cloud Security
- Industrial Control Systems (ICS) Security
- Mobile Application Security Testing (MAST)
- SaaS Governance

Survey Reports

- Cloud Adoption Survey Reports

Collaboration

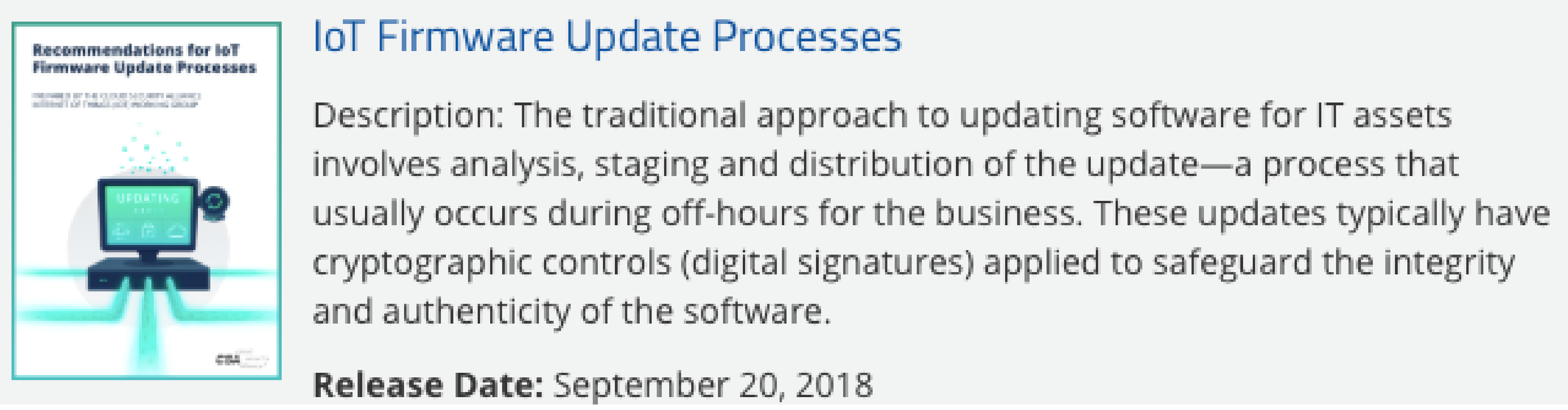
- Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud (STRATUS)

Recent Research Releases

All Free (as in beer) to download from CloudSecurityAlliance.org!

Guideline on Effectively Managing Security Service in the Cloud

This initiative aims to develop a research whitepaper, focusing on building up a cloud se
This whitepaper will serve as a guideline for cloud service providers to secure its cloud p
services to cloud users, for cloud users to select security qualified cloud service provide
cloud-based security products and services.



IoT Firmware Update Processes

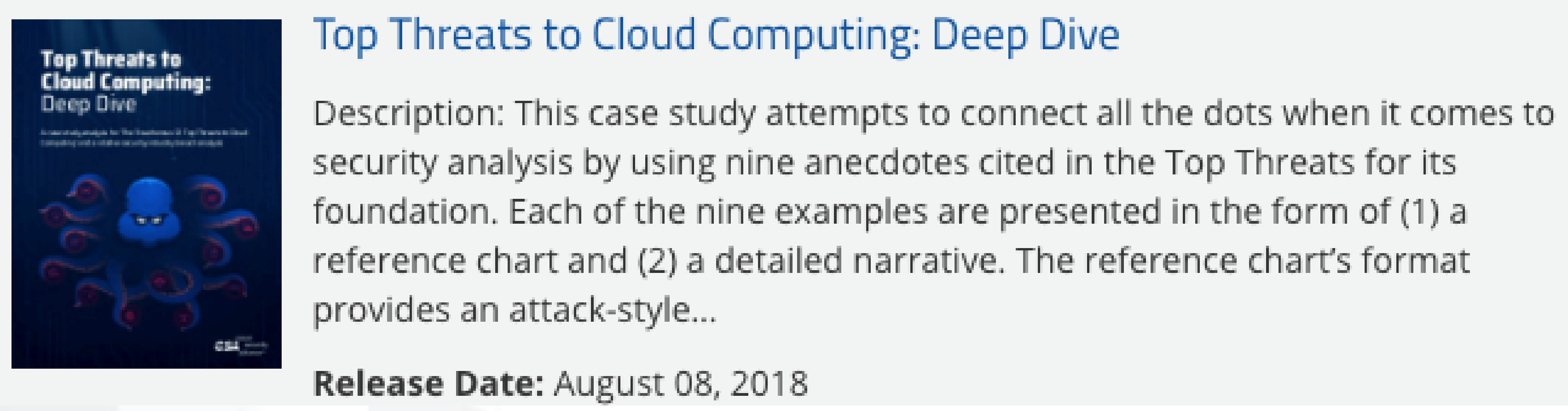
Description: The traditional approach to updating software for IT assets involves analysis, staging and distribution of the update—a process that usually occurs during off-hours for the business. These updates typically have cryptographic controls (digital signatures) applied to safeguard the integrity and authenticity of the software.

Release Date: September 20, 2018

CSA Malaysia FSI Report

Description: The "Cloud Adoption in the Malaysian Financial Services Industry (FSI) sector" survey was undertaken by CSA to understand and evaluate cloud adoption trends and concerns in the FSI in that country.

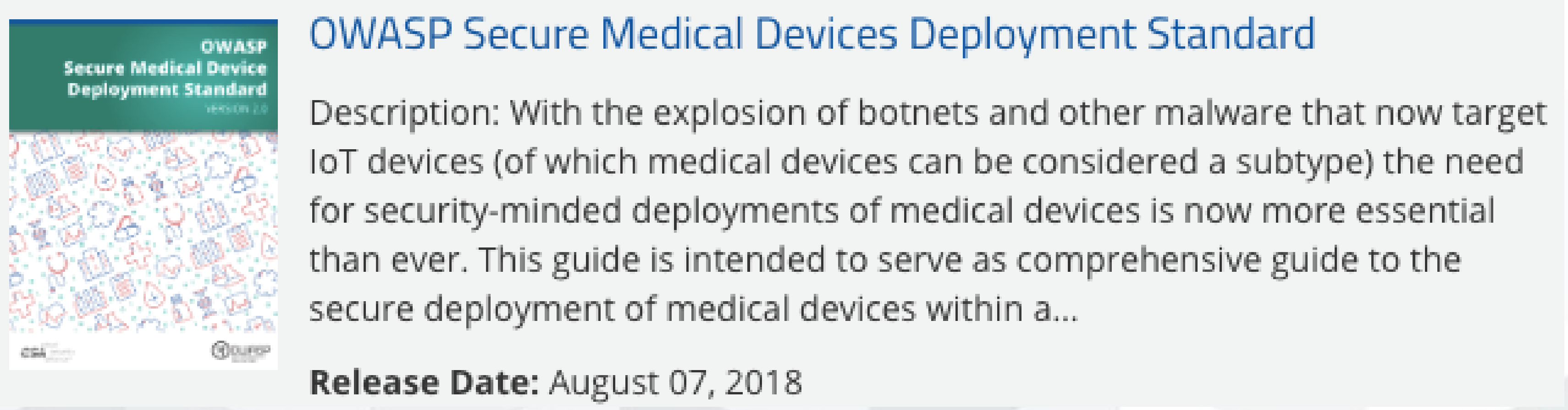
Release Date: August 20, 2018



Top Threats to Cloud Computing: Deep Dive

Description: This case study attempts to connect all the dots when it comes to security analysis by using nine anecdotes cited in the Top Threats for its foundation. Each of the nine examples are presented in the form of (1) a reference chart and (2) a detailed narrative. The reference chart's format provides an attack-style...

Release Date: August 08, 2018



OWASP Secure Medical Devices Deployment Standard

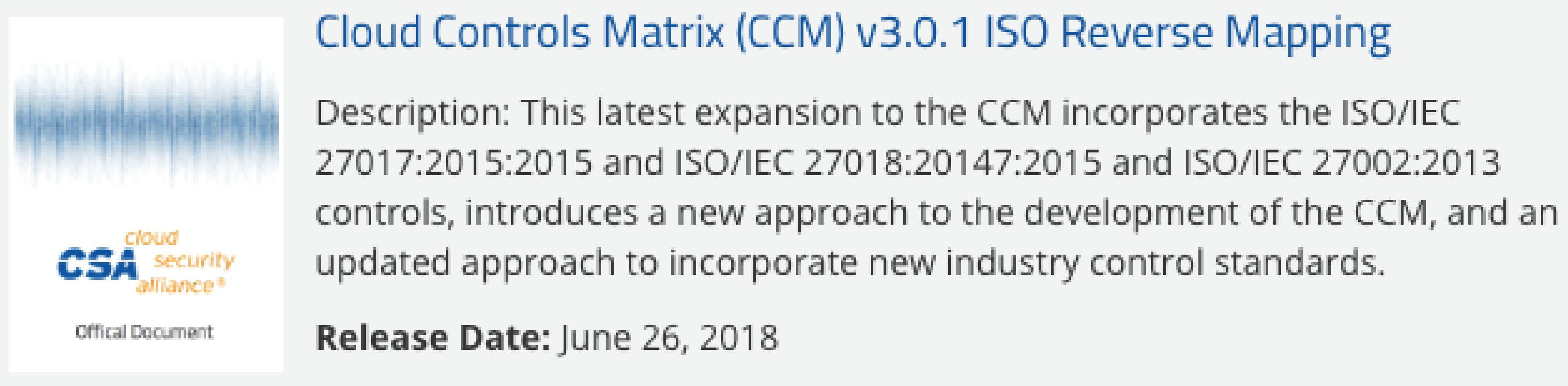
Description: With the explosion of botnets and other malware that now target IoT devices (of which medical devices can be considered a subtype) the need for security-minded deployments of medical devices is now more essential than ever. This guide is intended to serve as comprehensive guide to the secure deployment of medical devices within a...

Release Date: August 07, 2018

Cloud Security Alliance Code of Conduct for GDPR Compliance

Description: The CSA Code of Conduct is designed to offer both a compliance tool for GDPR compliance and transparency guidelines regarding the level of data protection offered by the Cloud Service Provider.

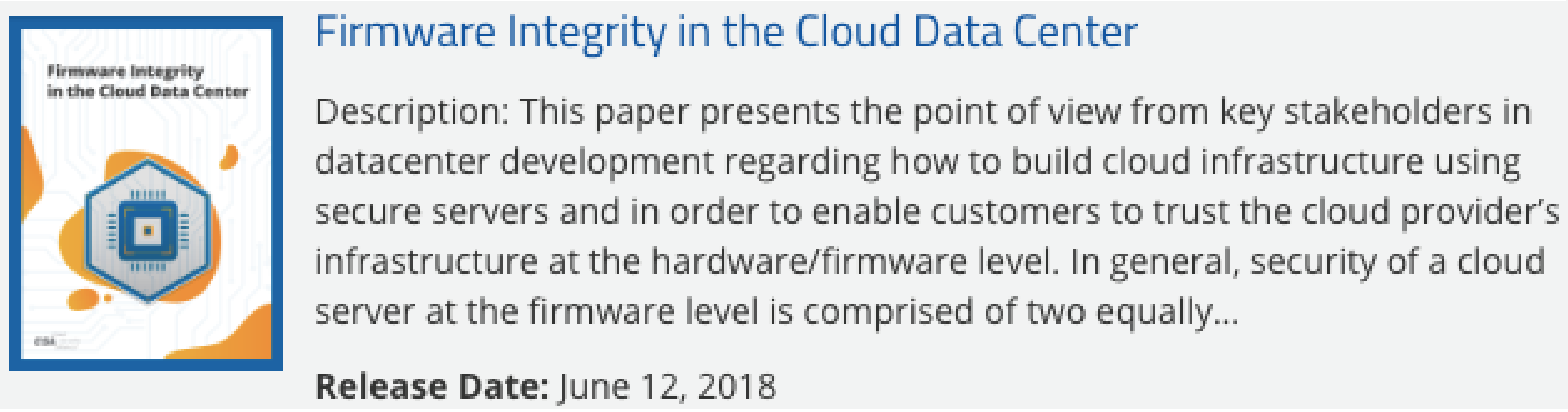
Release Date: July 10, 2018



Cloud Controls Matrix (CCM) v3.0.1 ISO Reverse Mapping

Description: This latest expansion to the CCM incorporates the ISO/IEC 27017:2015:2015 and ISO/IEC 27018:20147:2015 and ISO/IEC 27002:2013 controls, introduces a new approach to the development of the CCM, and an updated approach to incorporate new industry control standards.

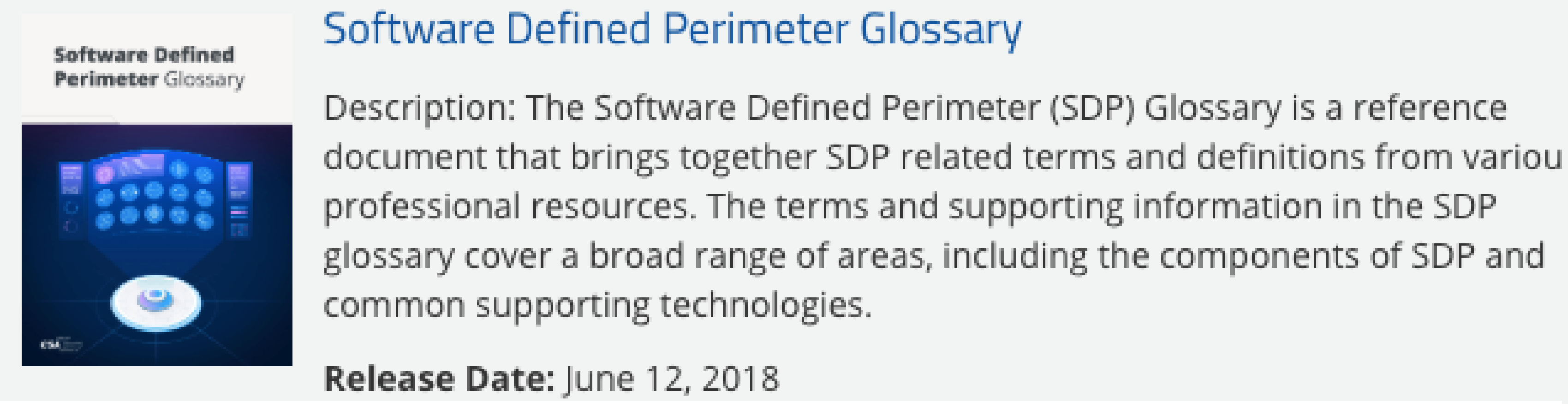
Release Date: June 26, 2018



Firmware Integrity in the Cloud Data Center

Description: This paper presents the point of view from key stakeholders in datacenter development regarding how to build cloud infrastructure using secure servers and in order to enable customers to trust the cloud provider's infrastructure at the hardware/firmware level. In general, security of a cloud server at the firmware level is comprised of two equally...

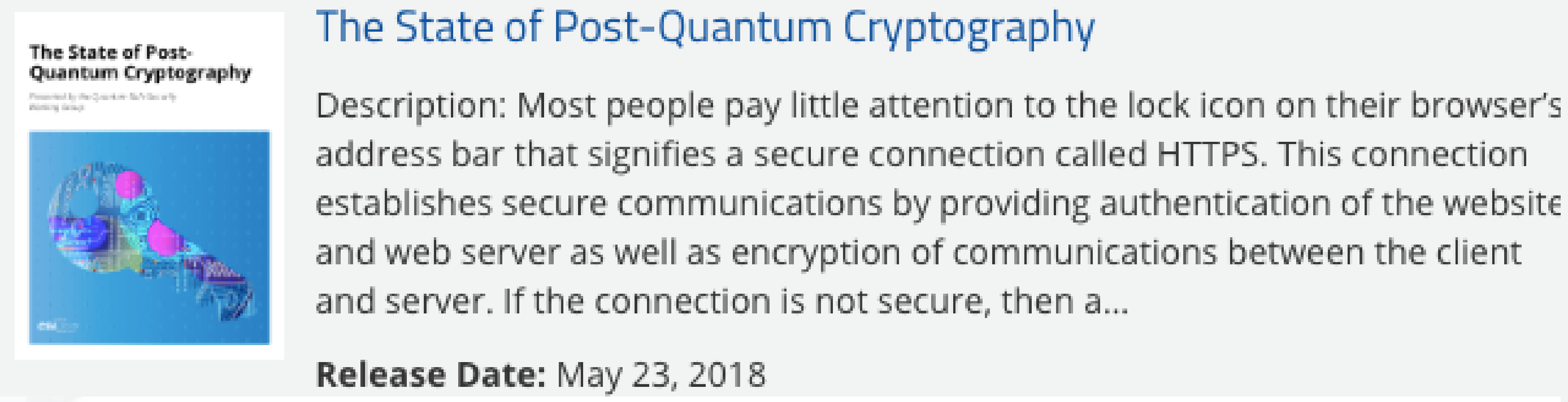
Release Date: June 12, 2018



Software Defined Perimeter Glossary

Description: The Software Defined Perimeter (SDP) Glossary is a reference document that brings together SDP related terms and definitions from variou professional resources. The terms and supporting information in the SDP glossary cover a broad range of areas, including the components of SDP and common supporting technologies.

Release Date: June 12, 2018



The State of Post-Quantum Cryptography

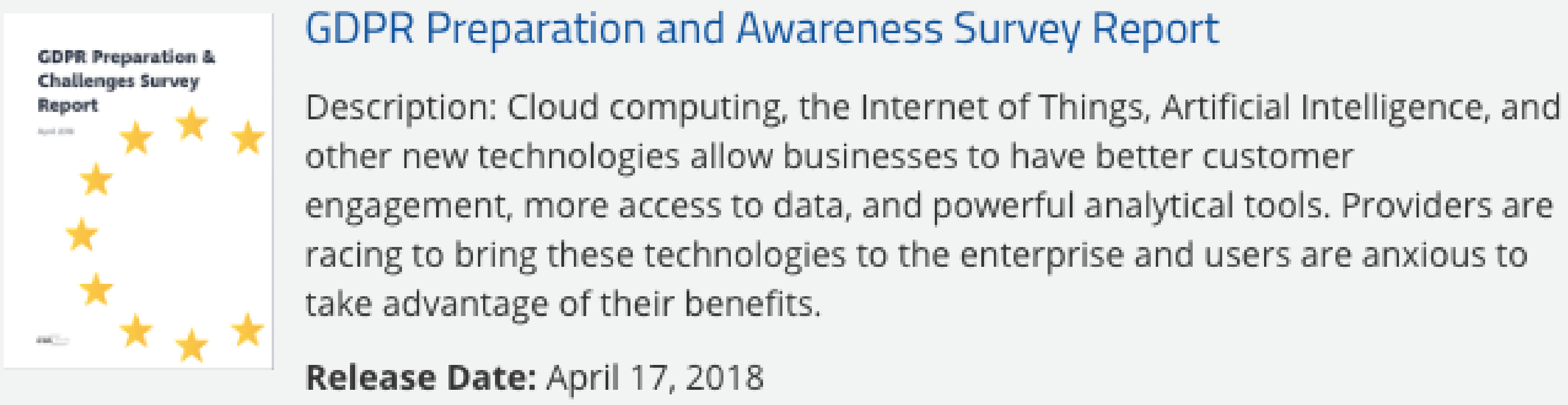
Description: Most people pay little attention to the lock icon on their browser's address bar that signifies a secure connection called HTTPS. This connection establishes secure communications by providing authentication of the website and web server as well as encryption of communications between the client and server. If the connection is not secure, then a...

Release Date: May 23, 2018

A Day Without Safe Cryptography

Description: Over the past fifty years, the digital age has sparked the creation of a remarkable infrastructure through which a nearly infinite variety of digital transactions and communications are executed, enabling businesses, education, governments, and communities to thrive and prosper. Millions of new devices are connecting to the Internet, creating, processing, and transferring digital information...

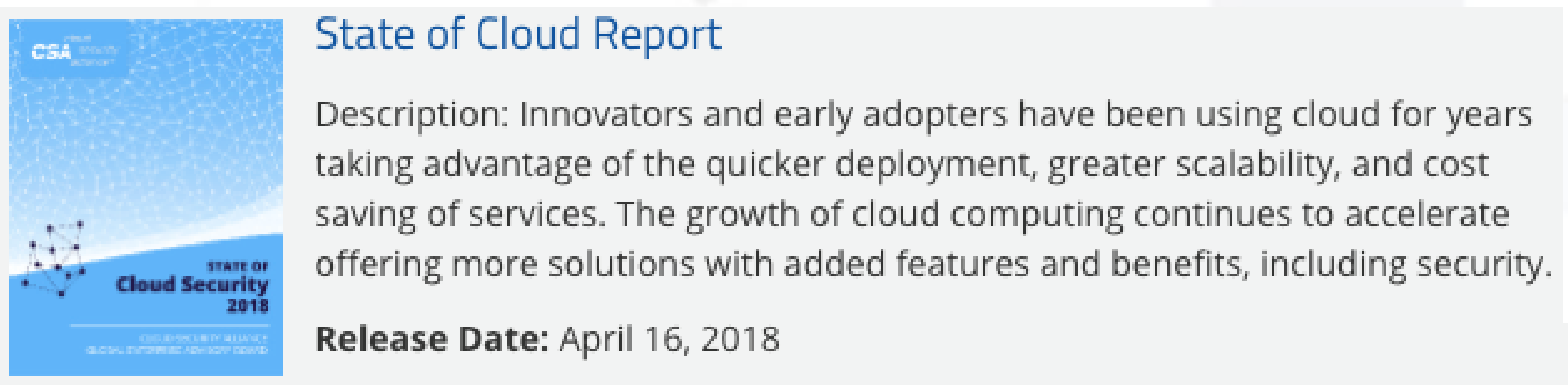
Release Date: April 19, 2018



GDPR Preparation and Awareness Survey Report

Description: Cloud computing, the Internet of Things, Artificial Intelligence, and other new technologies allow businesses to have better customer engagement, more access to data, and powerful analytical tools. Providers are racing to bring these technologies to the enterprise and users are anxious to take advantage of their benefits.

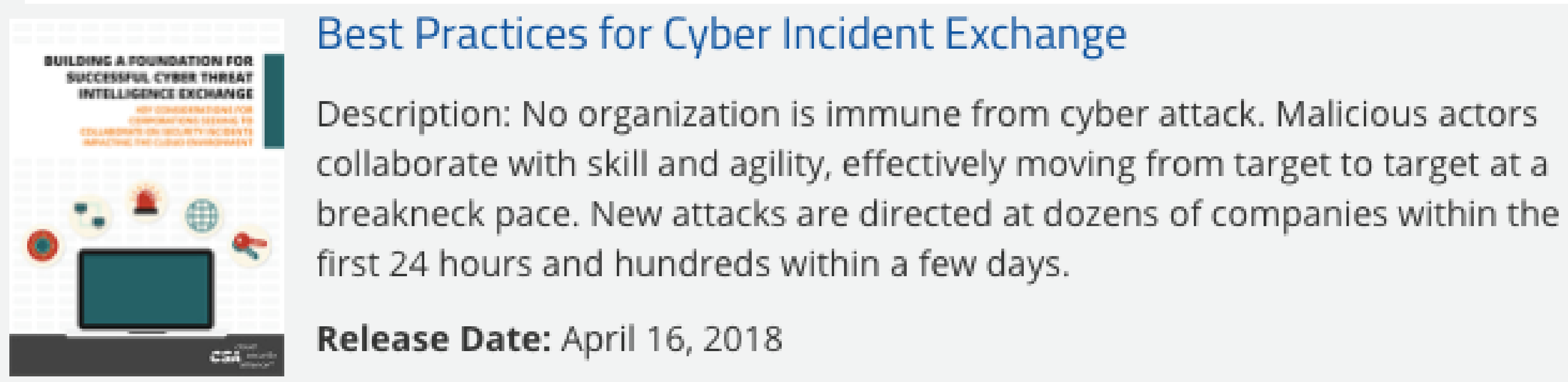
Release Date: April 17, 2018



State of Cloud Report

Description: Innovators and early adopters have been using cloud for years taking advantage of the quicker deployment, greater scalability, and cost saving of services. The growth of cloud computing continues to accelerate offering more solutions with added features and benefits, including security.

Release Date: April 16, 2018



Best Practices for Cyber Incident Exchange

Description: No organization is immune from cyber attack. Malicious actors collaborate with skill and agility, effectively moving from target to target at a breakneck pace. New attacks are directed at dozens of companies within the first 24 hours and hundreds within a few days.

Release Date: April 16, 2018

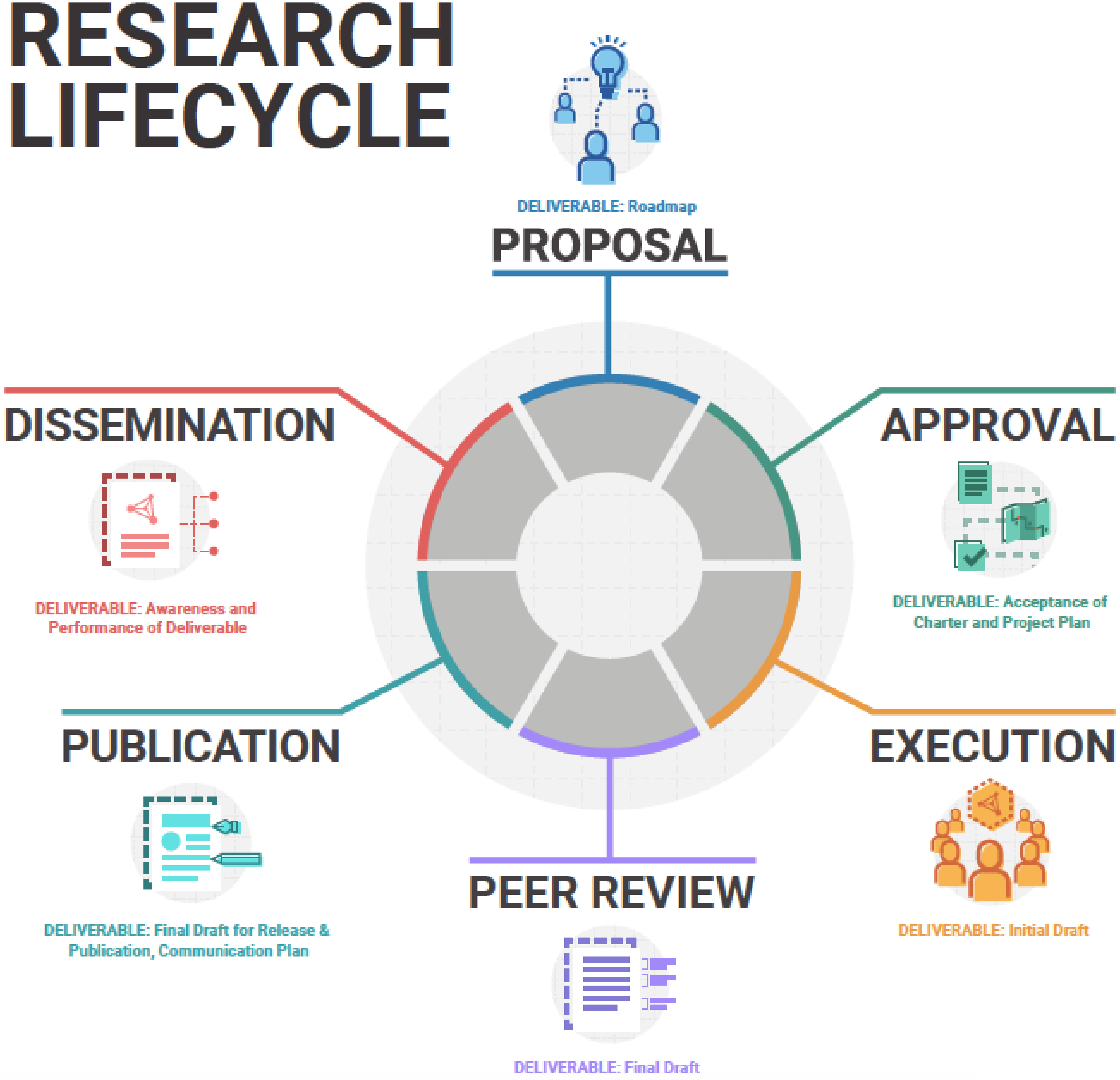
Using Blockchain Technology to Secure the Internet of Things

Description: In the last four years, technical experts, chief digital officers, marketing managers, journalists, bloggers and research institutions have discussed and promoted a new distributed model for secure transaction processing and storage using blockchain technology. IDC FutureScape predicted that by 2020, 20% of global trade finance will incorporate blockchain.

Release Date: February 13, 2018

https://cloudsecurityalliance.org/research/#_research-lifecycle

RESEARCH LIFECYCLE



DELIVERABLE: Roadmap

PROPOSAL

APPROVAL

DELIVERABLE: Acceptance of Charter and Project Plan

EXECUTION

DELIVERABLE: Initial Draft

PEER REVIEW

DELIVERABLE: Final Draft

PUBLICATION

DELIVERABLE: Final Draft for Release & Publication, Communication Plan

DISSEMINATION

DELIVERABLE: Awareness and Performance of Deliverable

CSA APAC cloud security
ASIA PACIFIC REGION alliance®

PEER REVIEW

The peer review process will be conducted to include the internal subgroup(s), working group(s), advisory groups, CSA commmunity, and public sources. (Typically 1-3 months.)

1-3 months

❶ WORKING GROUP PEER REVIEW

Draft of research artifact is sent to the working group for peer review.

❷ CSA PEER REVIEW

CSA peer review from Advisory Councils. Outreach begins for draft review by Marketing and PR.

❸ OPEN PEER REVIEW

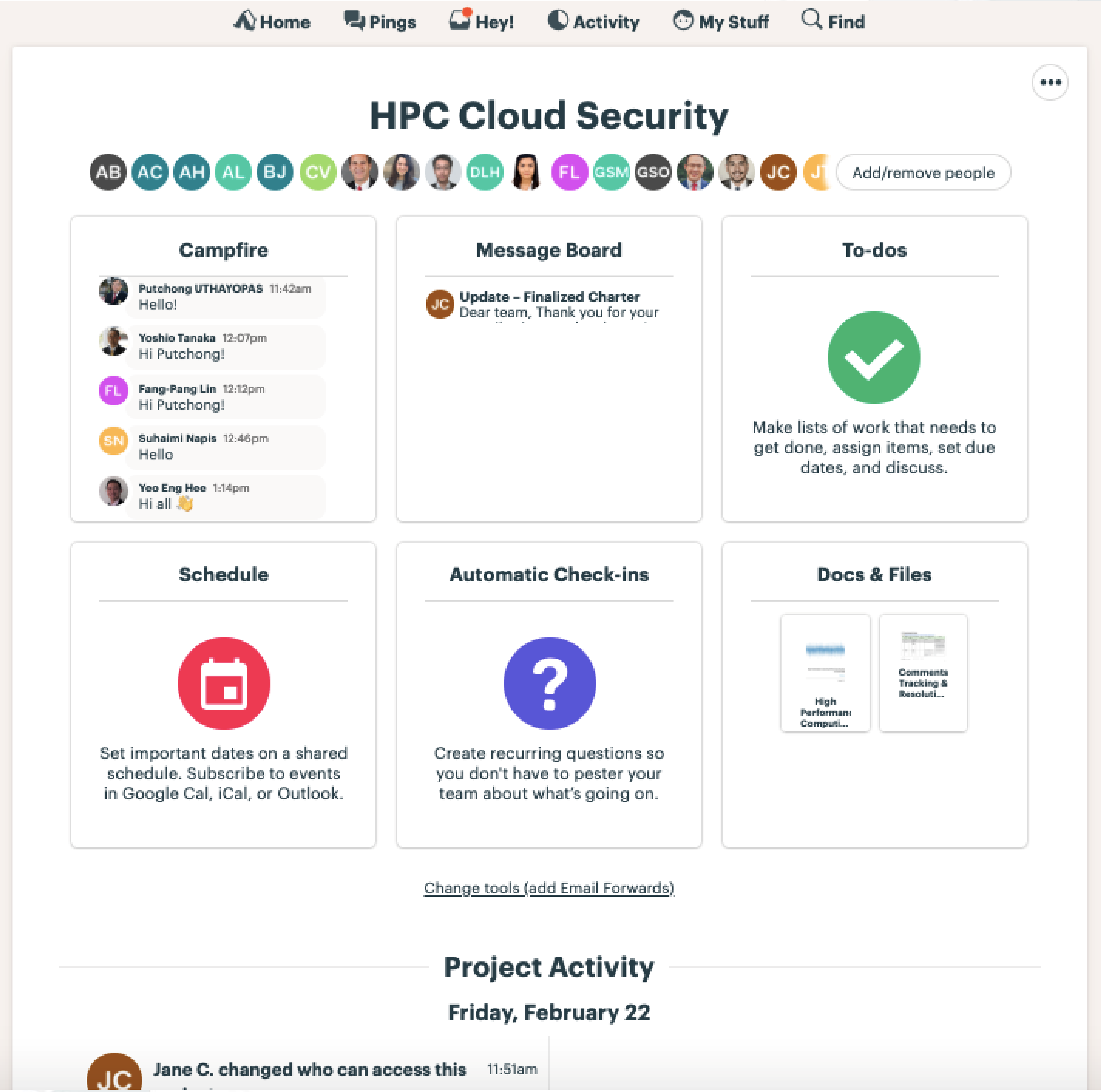
Draft is released to public for industry feedback

❹ INCORPORATE FEEDBACK

Compilation and deliberation of feedback into research artifact. (1 week minimum)

DELIVERABLE Final Draft

Basecamp


Home
Pings
Hey!
Activity
My Stuff
Find
AB AC AH AL BJ CV DLH FL GSM GSO JC JT
Add/remove people
High Performan Computi...
Comments Tracking & Resoluti...

HPC Cloud Security

Campfire

Putchong UTHAYOPAS 11:42am
Hello!

Yoshio Tanaka 12:07pm
Hi Putchong!

Fang-Pang Lin 12:12pm
Hi Putchong!

Suhaimi Napis 12:46pm
Hello

Yeo Eng Hee 1:14pm
Hi all 👋

Message Board

Update – Finalized Charter
Dear team, Thank you for your

To-dos

Make lists of work that needs to get done, assign items, set due dates, and discuss.

Schedule

Set important dates on a shared schedule. Subscribe to events in Google Cal, iCal, or Outlook.

Automatic Check-ins

Create recurring questions so you don't have to pester your team about what's going on.

Docs & Files

Change tools (add Email Forwards)

Project Activity

Friday, February 22

Jane C. changed who can access this 11:51am

Introduction to the HPC Cloud Security Working Group (WG)

HPC Cloud Security WG

Mission statement

To develop a holistic security framework for cloud infrastructure architected for high performance computing (HPC) needs, with the aim of securing where the cloud environment and HPC cross paths.

Organizations Represented in WG So Far

Supercomputing Facilities

1. European Organization for Nuclear Research (CERN)
2. King Abdullah University of Science and Technology (KAUST), Saudi Arabia
3. National Centre for High-Performance Computing (NCHC), Taiwan
4. National Computational Infrastructure (NCI), ANU, Australia
5. National Institute of Advanced Industrial Science and Technology (AIST), Japan
6. National Supercomputing Centre (NSCC), Singapore
7. Pawsey Supercomputing Centre, Australia
8. Research Organization for Information Science and Technology (RIST), Japan

Academic / Research / Gov Institutes

1. Institute for High Performance Computing (IHPC), A*STAR, Singapore
2. Kasetsart University (KU), Thailand
3. National University of Singapore (NUS)
4. National Electronics and Computer Technology Center (NECTEC), Thailand
5. Universiti Putra Malaysia (UPM)

Cloud Service Providers with HPC Offerings

1. Amazon Web Services (AWS)
2. Microsoft

Solution Providers

1. Checkpoint
2. Cray
3. Drootoo
4. Fujitsu
5. Netweb
6. Redhat
7. Rescale
8. Securosys

Background

- Increasing complexity of different types of workload has resulted in the diversity of infra architectures to serve them, with cloud environments now viable to process certain HPC workloads

- In addition, more workloads which are traditionally too sensitive to leave the on-prem infrastructure are now moving into the cloud in order to harness its benefits (eg. precision medicine, financial modelling)

- However, amongst all the demonstrated efficacies that cloud has brought about, researchers face certain challenges running HPC in a cloud environment

Technical Challenges

- Due to high performance requirements of HPC workloads, ‘close to metal’ operations are often demanded, stretching the processor’s core physical compute resource to its utmost capabilities. Running on a virtualized hypervisor may cause performance to suffer

- Whether high-speed interconnect is available also affects HPC’s performance

Security Challenges

- Increasingly, with pure HPC bare metal infra interacting with the cloud, coupled with the evolving threat landscape, there will be more opportunities for malicious attacks.

- However, high performance faces the peril of being compromised when precious resources are carved out for security protocols and processes

- The crossing of cloud and HPC environments often leads us to questions of how security in an HPC cloud environment can be implemented, enforced and ensured without the need to compromise performance

- The WG strives to provide recommendations that can answer these questions

WG Scope

The scope for the HPC Cloud Security working group includes, but is not limited to:

- Develop a set of security guidelines for cloud infrastructures architected for HPC needs
- Develop holistic security framework covering HPC cloud infrastructure and pure HPC bare metal infrastructure; and also on-premise infrastructure overflowing to public cloud infrastructures
- Develop reference models for secured HPC cloud implementation
- Share with other HPC thought leaders in the region

Additional Areas Suggested for the WG to Consider & Address

These were suggested during introductory calls with current WG members, or received as part of the open peer review process for the WG Charter:

- Clear definition of HPC – There is currently a broad definition, seen differently through the lens of HPC purists and CSPs
- Infrastructure security
- Network security
- Application security
- Identity management

Call for Participation in WG

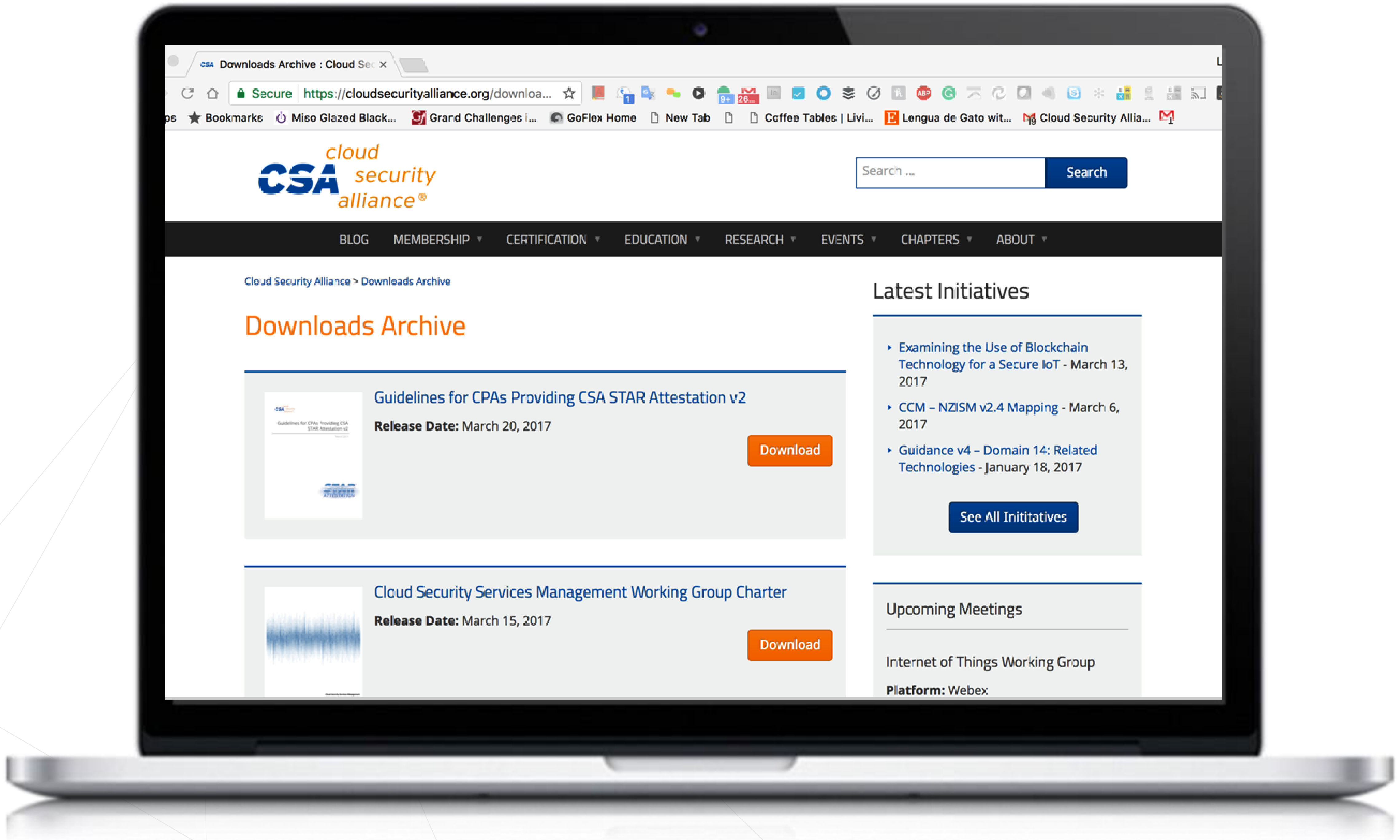
- We encourage HPC players from the international arena to join the WG

- Join us by submitting your info via https://goo.gl/KaAFfJ or contact csa-apac-research@cloudsecurityalliance.org

- The WG will hold similar sessions like this workshop in similar events around the world. Updates will be communicated on the WG's Basecamp and via https://www.csaapac.org

- We look forward to seeing you on the WG and at future events!

THANK YOU



Cloud Security Alliance > Downloads Archive

Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Download

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Download

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM – NZISM v2.4 Mapping - March 6, 2017
- Guidance v4 – Domain 14: Related Technologies - January 18, 2017

See All Inititatives

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

Contact CSA

Email: hzhuang@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

GDPR Resource center: https://gdpr.cloudsecurityalliance.org