Cloud Security Alliance
SDP Zero Trust Working Group Kickoff call - Sept 23 2020

Meeting Agenda

- **General overview – John Yeoh and Shamun Mahmud**
  - CSA Research Portfolio
  - Intro to SDP ZT WG Leadership
  - Intro to SDP, history, Spec v1 **(Bob Flores and Junaid Islam)**
- **Working Group Activities – TEAM**
  - SDP ZT Charter 2020-21
  - Bi-weekly calls
  - Quarterly updates (TBD)
  - Semi-annual in-person meetings (TBD)
- **Latest Publications**
  - SDP Architecture Guide – **Jason Garbis**
  - SDP and Zero Trust – **Juanita Koilpillai**
  - SDP as a DDoS Prevention Mechanism – **Juanita Koilpillai**
- **Business approach to COVID and associated risks - PANEL**
- **Current Roadmap**
  - SDP Design Specification v2.0 - **Junaid and Juanita**
  - POC: SDP and Zero Trust - **Juanita**
- **Future Topics**
  - Remote access topics such as: **SDP and 5G**
  - DHCP/DNS - as proposed
  - MFA and VPN using SDP DDoS Approach - as proposed
  - Vulnerability Assessments, CASB, SaaS Governance, Microsegmentation Governance
  - Privacy/security
- **Call for Action**
  - **Join the CSA SDP Zero Trust Working Group!**
  - Propose future topics/publications (See above “Future Topics”)
  - Participate in Zero Trust industry peering (ex: NIST 800-207, Circle, etc...)
  - Understand and discuss the latest trends in cloud and access services
  - Leverage authentication methodologies and Risk Management strategies in the cloud
  - Innovate from the cloud with SDP mechanisms

SDP Zero Trust WG Kick-Off Call

The SDP Zero Trust Working Group (WG) launched with the goal to develop a solution to stop network attacks against application infrastructure. With the adoption of cloud services the threat of network attacks against application infrastructure increases since servers can not be protected with traditional perimeter defense techniques.

Cloud Security Alliance CSA

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and organizations that offer qualified professional services based on CSA best practices.

In 2009, CSA released the Security Guidance for Critical Areas of Focus In Cloud Computing, providing a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. The following year, CSA launched the industry's first cloud security user certification, the Certificate of Cloud Security Knowledge (CCSK), the benchmark for professional competency in cloud computing security, along with the Cloud Controls Matrix (CCM), the world's only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations. By way of follow up, in 2015 together with (ISC)², CSA debuted the Certified Cloud Security Professional (CCSP) certification, representing the advanced skills required to secure the cloud.

CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA research prides itself on vendor neutrality, agility and integrity of results. CSA has a presence in every continent except Antarctica. With our own offices, partnerships, member organizations and chapters, there are always CSA experts near you. CSA holds dozens of high quality educational events around the world and online. Please check out our events page for more information.

OUR COMMUNITY

100,000+
INDIVIDUAL MEMBERS

75+
CHAPTERS

400+
CORPORATE MEMBERS

28+
ACTIVE WORKING GROUPS

30,000+
SUBSCRIBERS TO OUR WEBINAR SERIES

6,000+
RESEARCH VOLUNTEERS CONTRIBUTING

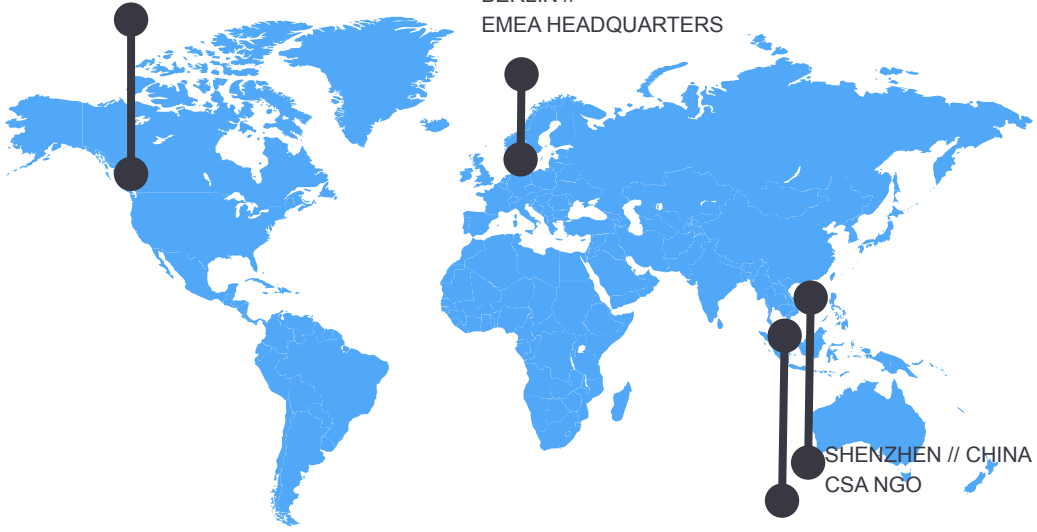
Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

2009
CSA FOUNDED

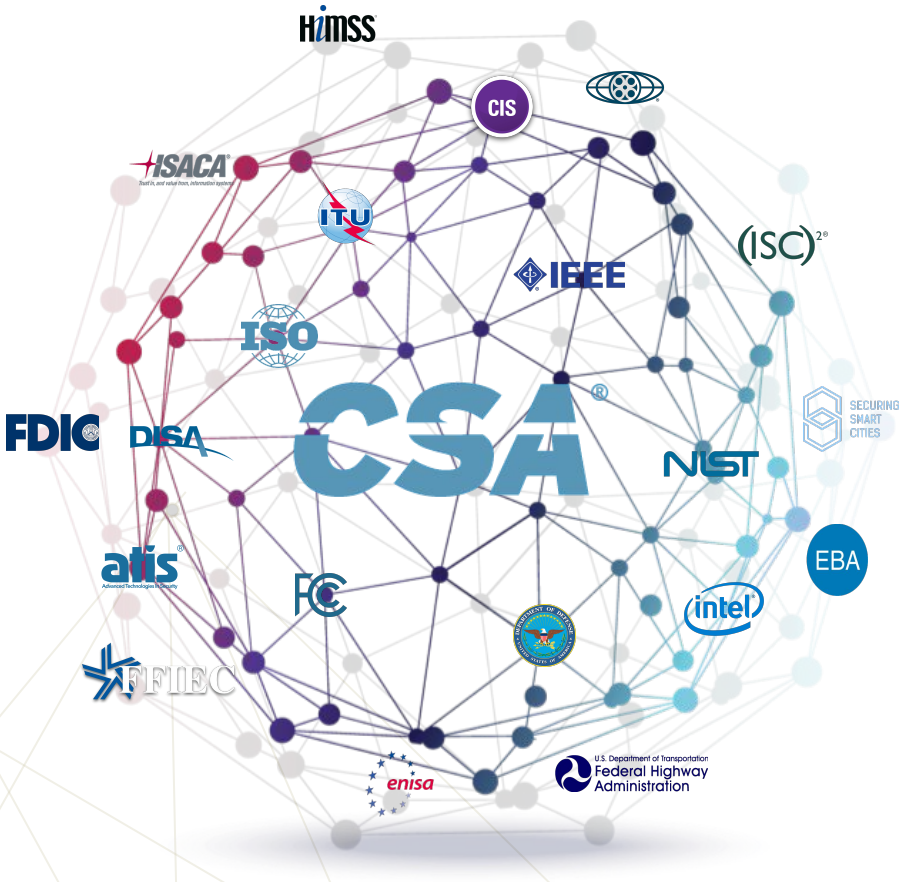
SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // EMEA HEADQUARTERS



SHENZHEN // CHINA CSA NGO

SINGAPORE // ASIA PACIFIC HEADQUARTERS



Industry Collaboration

FORMAL:

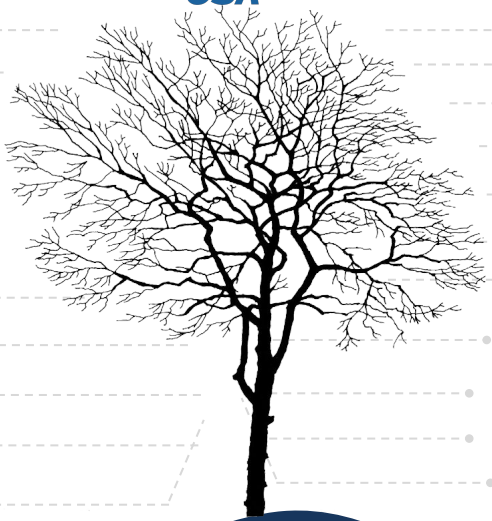
- ISO/IEC JTC 1 – IT and Cloud Security Techniques
- ITU-T – Procedures and standards in Telecom
- IEEE – Cybersecurity and Privacy Standards Committee
- NIST – Cloud Security Working Group
- FCC - Technological Advisory Committee on IoT
- DISA DoDIN (GIG) – Cloud Computing Services Guidance
- DoD IC - Cloud Computing Standards Focus Group
- ATIS - Packet Technology and Systems Committee on 5G
- CIS – Cloud Security Benchmarks
- Cloud Security Industry Summit – Executive Council of Cloud
- ENISA – EU funded research on Risk, Interoperability, SLAs, and more
- ISC2 – Training and Education Partner for Cloud Security Certification
- ISACA – Continuing Education Partner for IT Certification
- CSA Corporate Members – Commissioned work to explore trending topics
- And many others

INFORMAL:

MPAA, Security Smart Cities, US Federal Highway Administration, HIMSS, HC3, FFIEC, FDIC, OCC, EBA, UL, and more

CSA RESEARCH

ACTIVE PUBLIC Working Groups



- INTERNATIONAL STANDARDS
- FINANCIAL SERVICES
- HEALTHCARE INFORMATION
- SERVERLESS
- CONTAINERS & MICROSERVICES
- DEV(SEC)OPS
- SDP ZERO TRUST
- ERP SECURITY
- CLOUD KEY MANAGEMENT
- OPEN CERTIFICATION FRAMEWORK
- CLOUD COMPONENT SPECIFICATIONS
- ENTERPRISE ARCHITECTURES
- CLOUD CONTROLS MATRIX
- ARTIFICIAL INTELLIGENCE
- QUANTUM SAFE SECURITY
- BLOCKCHAIN
- INTERNET OF THINGS
- INDUSTRIAL CONTROLS SYSTEMS
- MOBILE APPLICATION SECURITY
- INCIDENT RESPONSE
- CYBER INTELLIGENCE EXCHANGE
- TOP THREATS
- PRIVACY LEVEL AGREEMENTS
- SECURITY SERVICES MANAGEMENT
- SAAS GOVERNANCE
- SECURITY AS A SERVICE

EDUCATION

THOUGHT LEADERSHIP

TOOLS & STANDARDS

COLLABORATION

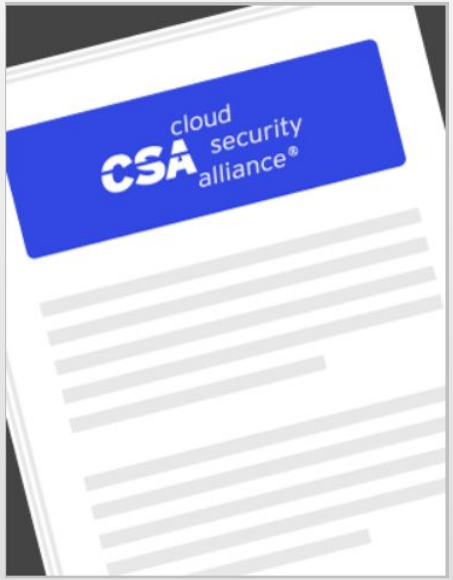
BEST PRACTICES & SOLUTIONS

SDP Zero Trust Leadership

- **Co-Chairs**
  - Bob Flores – Applicology Incorporated
  - Jason Garbis – SVP of Products, Appgate
  - Junaid Islam – 5G Security Advisor at National Spectrum Consortium
- **Technical Advisor**
  - Juanita Koilpillai – Founder and CEO, Waverley Labs
- **Cloud Security Alliance Research**
  - Shamun Mahmud - Sr. Research Analyst
  - John Yeoh - VP of CSA Global Research

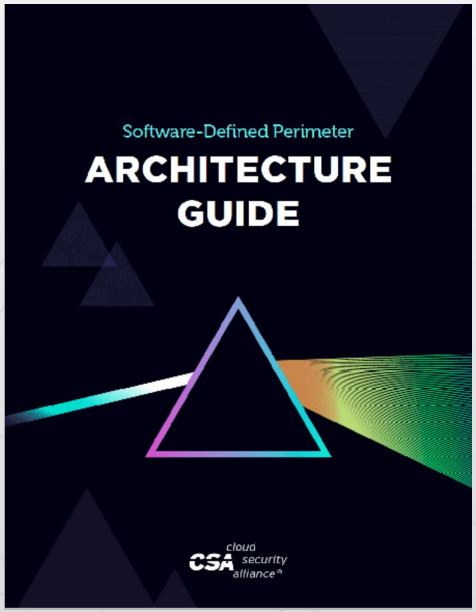
SDP ZT Working Group Activities – Shamun Mahmud

- SDP Zero Trust Charter 2020-21
- CSA Circle SDP Zero Trust Working Group
- SDP ZT WG Monthly calls
- Semi-annual in-person meetings
- Quarterly regulator updates



Latest Publications - Jason Garbis

- SDP Architecture Guide
  - **May 7th, 2019**



Software Defined Perimeter (SDP) Architecture Guide is designed to leverage proven, standards-based components to stop network attacks against application infrastructure. The architecture guide will help increase awareness and adoption of SDP, improve understanding of how SDP can be used in different environments, and help enterprises successfully deploy SDP solutions based on the architecture recommendations.

Latest Publications - Juanita Koilpillai

- SDP and Zero Trust
  - **May 27, 2020**

A Zero Trust implementation using Software-Defined Perimeter enables organizations to defend new variations of old attack methods that are constantly surfacing in existing network and infrastructure perimeter-centric networking models. Implementing SDP improves the security posture of businesses facing the challenge of continuously adapting to expanding attack surfaces that are increasingly more complex. This paper will show how SDP can be used to implement ZTNs and why SDP is applied to network connectivity, meaning it is agnostic of the underlying IP-based infrastructure and hones in on securing all connections using said infrastructure - it is the best architecture for achieving Zero Trust.

Latest Publications - Juanita Koilpillai

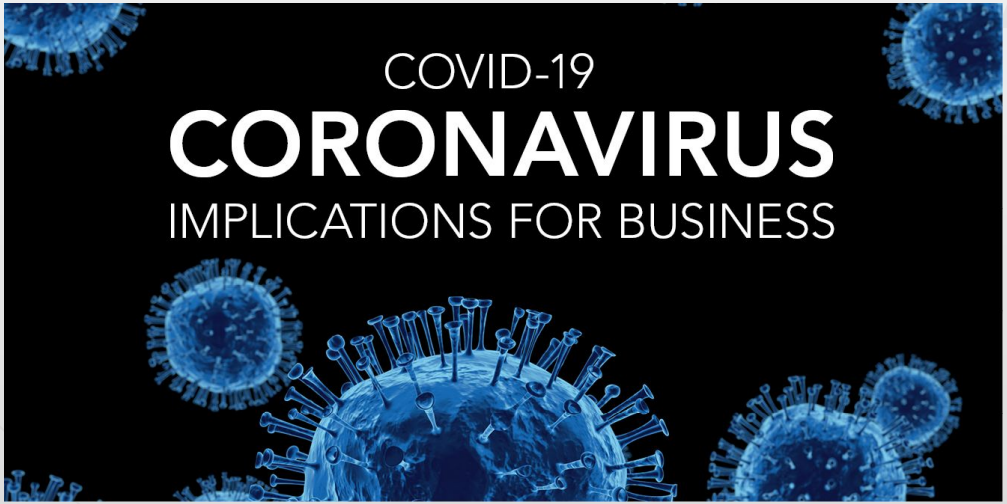
- SDP as a DDoS Preventative Mechanism
  - **October 27, 2019**

Mission:

- The primary goal of this document is to increase the awareness and understanding of SDP as a tool to prevent DDoS attacks by demonstrating its efficiency and effectiveness against several well-known attacks, including HTTP Flood, TCP SYN, and UDP Reflection.

Covid-19 Associated Risks - PANEL

- Business approach to Covid-19 and associated risks**. Such as:** Remote work, Mobile



Current Roadmap

- SDP Design Specification v2.0 – Juanita, Jason and Junaid
- POC - SDP Use Case study - Juanita

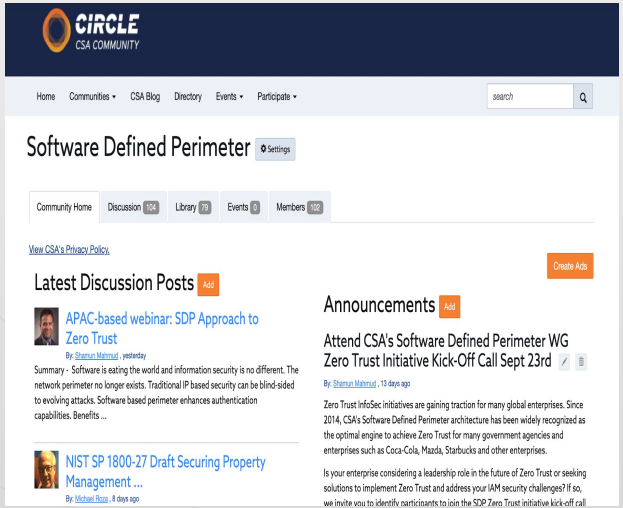
Future Topics - Join the Discussion

- Remote access arenas such as: SDP and 5G
- SPA-everywhere (ex: Deny-all FW)
- SDP and integration ID and authentication
- Microsegmentation Security
- SDP vendor capabilities survey, findings…

Call for Action

- **Join the CSA SDP Zero Trust Working Group!**
  - Next meeting October 7th 1:00 PM PT: https://cloudsecurityalliance.zoom.us/j/94151107820

- **Participate in Zero Trust industry peering.**
  - https://cloudsecurityalliance.org/research/contribute/

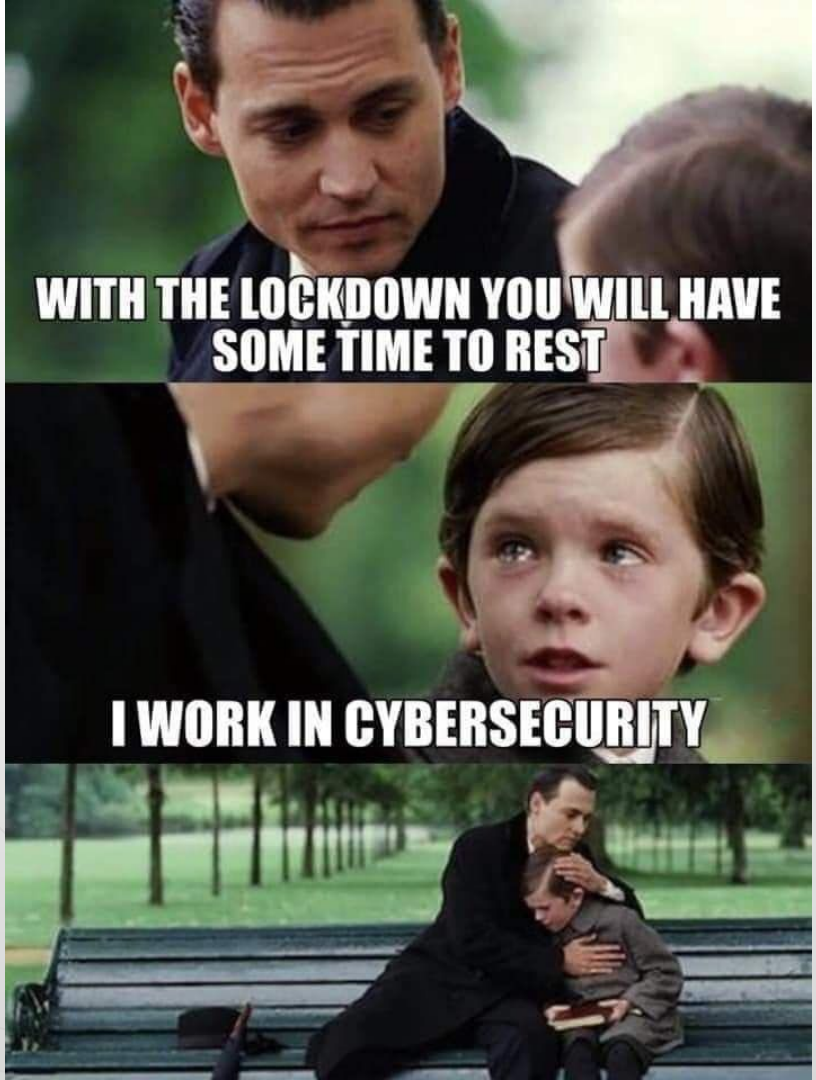


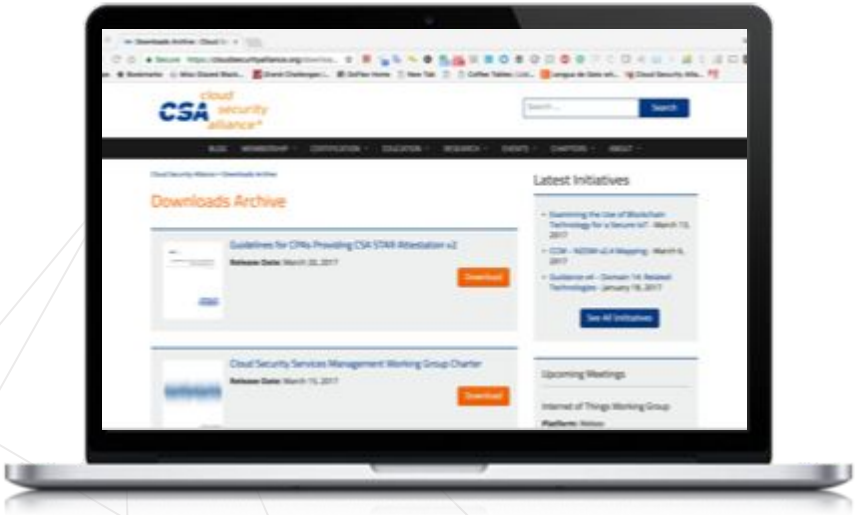
CIRCLE
CSA COMMUNITY

cloud security alliance®

Call for Action

- **Understand and discuss the latest trends in cloud and access services.**
  - Circle SDP Zero Trust Working Group
- **Leverage SDP methodologies and Zero Trust strategies in the cloud.**
  - SDP Architecture Guide v2.0
  - SDP and Zero Trust
- **Innovate from the cloud with SDP security technique.**
  - SDP as a DDoS Prevention Mechanism


WITH THE LOCKDOWN YOU WILL HAVE SOME TIME TO REST
I WORK IN CYBERSECURITY



Contact CSA Research

Email: research@cloudsecurityalliance.org

Twitter: @CloudSA

Overview: www.cloudsecurityalliance.org/research

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

Supplemental slides

Further details that elucidate

Working Groups (WGs)

The CSA maintains Working Groups across 36 domains of Cloud Security. Some WGs are dormant

Big Data	Blockchain/Distributed Ledger	Cloud Component Specifications
Cloud Controls Matrix	Cloud Data Center Security	Cloud Data Governance
Cloud Security Services Management	Cloud Vulnerabilities	CloudAudit
CloudCISC	CloudTrust	CloudTrust Protocol
Consensus Assessments	Containers and Microservices	Enterprise Architecture
Enterprise Resource Planning (ERP) Security	Financial Services Stakeholder Platform	Health Information Management
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

SDP Working Group Deliverables

Recent (and not-so-recent)

1) SDP Glossary v2.0. Q2 2018 release
2) Architectural Guidance v2.0. Q1 2019 release
3) SDP A&A Poll/survey blog article. Q2 2019 release
4) SDP as a DDoS Preventive Mechanism. Q3 2019 release
5) SDP and Zero Trust. *Q2 2020 release*
6) SDP Specification v2.0. *Q4 2020 release*

Further… Call for Papers (TEAM)

Ongoing (briefings available)

1) Open Source DDoS Initiative

SDP Working Group Initiatives explained

Status: Ongoing. Briefings: Currently Available

1) Open Source DDoS Initiative

1) **Objective:** Research SDP as a high speed Internet-based packet filter
2) **Application:** Enable access to mission critical sites during DDoS attacks

SDP News

What is SDP and Why Do I need it?
https://searchnetworking.techtarget.com/answer/What-is-a-software-defined-perimeter-and-do-I-need-it

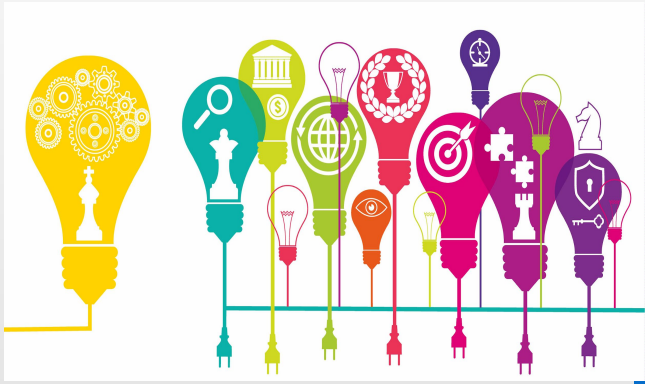
SDP or VPN: Which is better to secure remote access?
https://channels.theinnovationenterprise.com/articles/sdp-vs-vpn-which-is-better-to-secure-remote-access

Why Security Needs a Software-Defined Perimeter
https://www.darkreading.com/why-security-needs-a-software-defined-perimeter/a/d-id/1332666

Software-defined Perimeter: The Pathway to Zero Trust
(IN)Security Magazine
https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-58.pdf

Searching for the perimeter in cloud security: From microservices to chaos
Support of SDP model from industry experts
http://www.zdnet.com/article/the-old-software-fortress-weathers-the-storm-of-supreme-chaos/

Software Defined Perimeter (SDP) Market Technology Status, Application, Types, Trending Analysis 2017 to 2022
Current SDP vendors and market growth
https://www.newsient.com/software-defined-perimeter-sdp-market-technology-status-application-types-trending-analysis-2017-2022/126067



Thank You For Contributing!

SDP Co-Chair

Bob Flores
Jason Garbis
Junaid Islam

SDP Technical Advisor

Juanita Koilpillai

CSA Global Research

Shamun Mahmud
John Yeoh