The Future of Application Data Security: PCI and Beyond

Presenters:

Ed Adams, Security Innovation
Kara Gunderson, Citgo Petroleum
Marc Punzirudu, ControlScan

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 7 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: **info@conexxus.org**

CONEXXUS
solve forward

Presenters

Conexxus Host

Allie Russell
Standards Coordinator
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Panelists

Ed Adams – CEO, Security Innovation
Kara Gunderson – POS Manager, CITGO Petroleum
Marc Punzirudu – VP, Security Consulting Services, ControlScan

Panel Moderator

Sam Pfanstiel – Director, Security Consulting Services, ControlScan

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
March 18, 2020	The Future of Application Data Security: PCI and Beyond	Ed Adams Kara Gunderson Marc Punzirudu	Security Innovation CITGO ControlScan
April 2, 2020	Presentation by GS1	Liz Sertl	GS1
April 2020	Ransomware protection and how a managed security service provider can help oil & gas retailers from being the next target	Ajith Edakandi	Hughes Network
May 2020	POS Managed Service Program	TBD	Joint MNSP's
June 2020	Penetration Testing	Geoff Vaughan	Security Innovation

CONEXXUS
solve forward

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
July 2020	PCI DSS 4.0	Troy Leach	PCI SSC
August 2020	Vulnerability & Patch Management—Retail Operations	TBD	POS Vendors
September 2020	TBD	Scott Cheek	SageNet

CONEXXUS
solve forward

2020 Conexxus Annual Conference

April 26 – April 30, 2020

Loews Ventana Canyon
Tucson, AZ

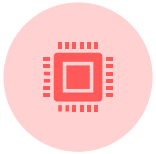
More about Sponsorship Opportunities & Registration:
www.conexxus.org/2020ac

Conexxus thanks our 2020 Annual Diamond Sponsors!

Bulloch Technologies Inc. www.bullochtech.com
Cybera
Diebold Nixdorf
Gilbarco Veeder-Root
Hughes An EchoStar Company
NACS
NCR
Security Innovation
Soundpayments Integration Made Easy
Stuzo

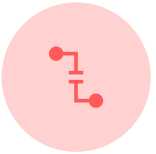
CONEXXUS solve forward

Software Security Threats to C-Stores



Memory-scraping malware

Ransomware on PCs, servers and POS systems



External attacks (from outside the environment)

Misconfigured network components (firewalls, routers and wireless access points)

Targeted attack from cybercriminals against infrastructures

Third-party software (POS systems or ISV software)

CONEXXUS solve forward

Other Threats to C-Stores

- Fines from card associations for breaches
- Costs of PCI DSS Forensics Investigations (PFI)
- Reputation / brand damage
- State and local privacy laws

CONEXXUS solve forward

Application Security for C-Stores

- Internal Vulnerability Management
- Legal Recourse (Contracting, SLA, Right to Audit)
- Custom Software Development
- Network and Application Security (WAF, RASP)
- Managed Security Providers (UTM)
- Service Provider Vulnerabilities

CONEXXUS solve forward

Application Security for Vendors

And merchants with custom apps!

- Governance
- Engineering
- Data Management
- Communications
- Software Lifecycle

Security Strategy, Protection Mechanisms, Operations, Management

CONEXXUS solve forward

PCI Trends and Concerns

- Over half of merchants claim to be in compliance, but are not.
  - Large merchants being assessed by a QSA have some amount of oversight. For Level 4 merchants, there's no way to determine how many simply checked yes to the questions and submitted the SAQ.
  - Regardless of PCI DSS, number of breached entities and breached records.
  - First decrease in the most recent Verizon breach report, but number of breached records is actually increasing

Recent PCI Changes for AppSec

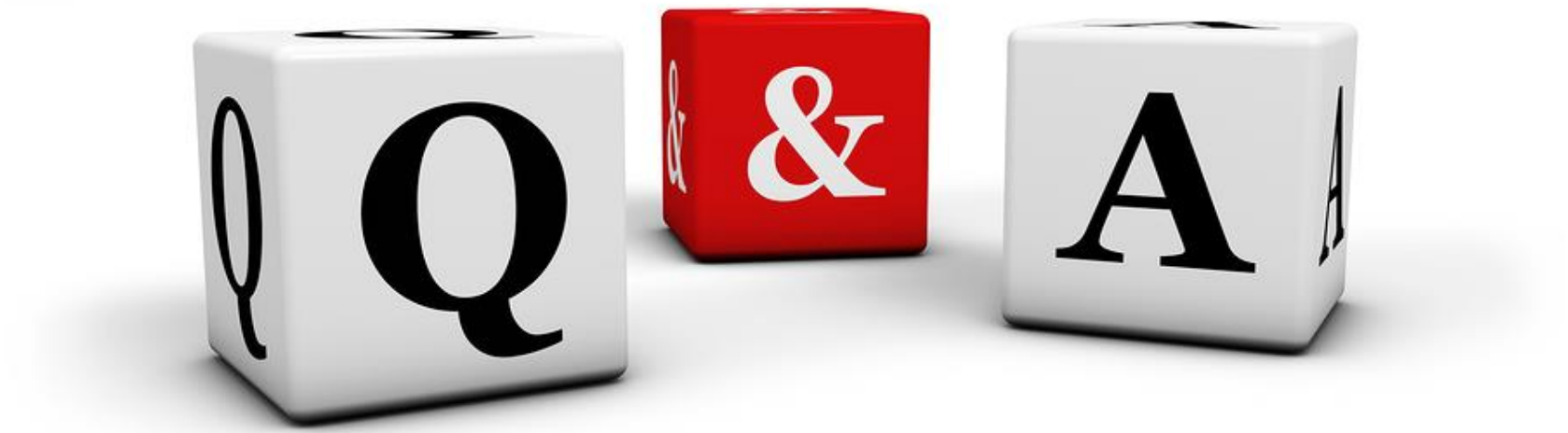
- SSF 1.0
  - Secure Software
  - Secure SLC
  - Replaces PA-DSS

- Framework for entire lifecycle
- Still requires QIR
- Eligible for commercial applications only
- Future modules may support SaaS, PII, Cloud, P2PE, etc., etc.

Other PCI Changes for AppSec

- PCI DSS 4.0
- P2PE 3.0
  - Descoping applications
- SPOC, CPOC, 3DS, PIN, TSP, etc.

- Focus on:
  - Data/Asset identification
  - Scoping
  - Automated testing
  - Cloud guidance on microservices / FaaS



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.