Application Security 101

Presenter:

Denis Sheridan, Synopsys
Agenda

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

This webinar is being recorded and will be made available in approximately 15 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
Presenters

Conexxus Host
Allie Russell
Conexxus
arussell@conexxus.org

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

Speakers
Denis Sheridan
Managing Principal, Synopsys
deniss@synopsys.com
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
<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 24, 2019</td>
<td>Who’s Watching Your Network? What you should know about Managed Detection &amp; Response (MDR)</td>
<td>Mark Carl</td>
<td>ControlScan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tom Callahan</td>
<td></td>
</tr>
<tr>
<td>March 21, 2019</td>
<td>Proactive Defense in Depth</td>
<td>Brett Stewart</td>
<td>Acumera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeWayne Mangan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mark Palmer</td>
<td></td>
</tr>
<tr>
<td>June 27, 2019</td>
<td>Web Payment Aspirations</td>
<td>Ian Jacobs</td>
<td>W3C</td>
</tr>
<tr>
<td>July 25, 2019</td>
<td>Skimming</td>
<td>Linda Toth</td>
<td>Conexxus NACS CITGO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paige Anderson</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Caleb Burke</td>
<td></td>
</tr>
<tr>
<td>August 8, 2019</td>
<td>Application Security 101</td>
<td>Denis Sheridan</td>
<td>Synopsys</td>
</tr>
</tbody>
</table>
## 2019-2020 Conexxus Webinar Schedule

<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 29, 2019</td>
<td>Don’t Get Phished!! Train Your Employees To Avoid Ransomware</td>
<td>Geoffrey Vaughan Ed Adams</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>September 26, 2019</td>
<td>Updated Data Science Presentation</td>
<td>Ashwin Swamy Thomas Duncan</td>
<td>Omega ATC Omega ATC</td>
</tr>
<tr>
<td>October, 2019</td>
<td>Easy PCI—How to Make PCI &amp; Attestation Easier</td>
<td>Ajith Edakandi</td>
<td>Hughes</td>
</tr>
<tr>
<td>November, 2019</td>
<td>EMV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>December, 2019</td>
<td>Applicability of PCI DSS requirements for Merchants and MNSP’s</td>
<td>Sam Pfanstiel</td>
<td>ControlScan</td>
</tr>
<tr>
<td>January, 2020</td>
<td>TBD</td>
<td>TBD</td>
<td>Cybera</td>
</tr>
</tbody>
</table>
Conexxus thanks our 2019 Annual Diamond Sponsors!

mSHIFT.  Relevant. Mobile. Solutions.
Stuzo
Diebold Nixdorf
Wex
Hughes
An EchoStar Company
Gilbarco Veedere-root
Cybera
Security Innovation

TECHEDGE
Booth # 3755

NACS Show
October 1-4, 2019
Atlanta, GA
Application Security 101

Presenter:

Denis Sheridan, Synopsys
Application Security 101

• More than just scanning/testing
• Building software securely
• Security as part of software development lifecycle
Today’s Goal

• Raise awareness among builders and buyers of software
• Breadth not depth… but please interrupt me and ask questions 😊
SECURE SDLC OVERVIEW
Generic SDLC

- App idea
- Design solution
- Code it
- Test it
- Ship it
Generic Secure SDLC

- Abuse cases
- Threat modeling
- Secure code review
- Security testing
- Security monitoring
Security Methodology

• “Think like an attacker” mindset
• Identify vulnerabilities and break assumptions
• Automated and manual approaches
SECURE SDLC ACTIVITIES
Abuse Cases

- Malicious complement to use cases
- Identify security concerns before solution is designed and coded
Threat Modeling

• Map out the system and where/how data flows between parts
• Identify missing or insufficient security controls
Secure Code Review

- Static Application Security Testing (SAST)
- IDE scanning versus build integration
- Reverse engineering*
Open Source Software

• Running a lot of code you didn’t write
• Raises both legal and security concerns
• Of particular interest during mergers and acquisitions
Security Testing

- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)
- Fuzz Testing
- Penetration Testing
- Post-deployment testing
- Red Team
Operational Security

• Web Application Firewall (WAF)
• Runtime Application Self-Protection (RASP)
• Code protections
• Bug bounty programs and responsible disclosure
BRINGING IT ALL TOGETHER
Managing Risk

• Ensure the right activity was performed to address your concern
• Tie findings back to business impact
• Ability to conduct all assessment types depends on producer-consumer relationship
App Sec Program

• Company-defined approach to application security
• Balance security and speed to market
• Adapt to changes in development landscape
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Profile: Conexxus.org
• Follow us on Twitter: @Conexxxusonline
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.
Images

- https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/fb10e181-7a4d-4ceb-98ab-45ac18906291.png
- https://assets.njspotlight.com/assets/18/0410/2345
- https://duo.com/assets/img/blogv2/dasmm-model.png
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRSBRHYDb2u87Zqd4Avmntn23vvU_vAMKTZg6URgO2xMfMg0_pBI