# Application Security 101

Presenter:

Denis Sheridan, Synopsys

CONEXXUS
solve forward

# 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

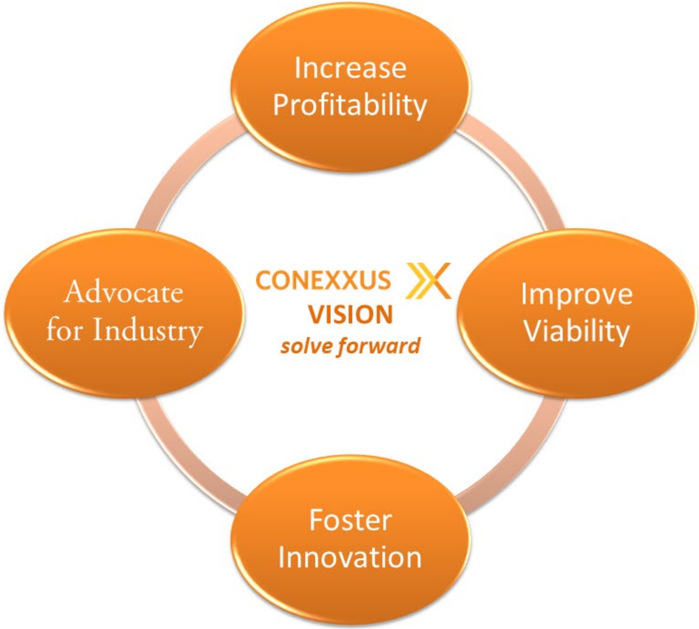
Denis Sheridan

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



# 2019 Conexxus Webinar Schedule

| Month/Date | Webinar Title | Speaker | Company |
|---|---|---|---|
| January 24, 2019 | Who’s Watching Your Network?<br>What you should know about Managed Detection & Response (MDR) | Mark Carl<br>Tom Callahan | ControlScan |
| February 28, 2019 | Protect Your Business: PCI Resources for Securing Payment Data | Elizabeth Terry | PCI Security Standards Council |
| March 21, 2019 | Proactive Defense in Depth | Brett Stewart<br>DeWayne Mangan<br>Mark Palmer | Acumera |
| May 30, 2019 | Firewalls, LANS & WANS<br>The Basics, The Benefits and The Security! | Simon Gamble | Mako Networks |
| June 27, 2019 | Web Payment Asipirations | Ian Jacobs | W3C |
| July 25, 2019 | Skimming | Linda Toth<br>Paige Anderson<br>Caleb Burke | Conexxus<br>NACS<br>CITGO |
| August 8, 2019 | Application Security 101 | Denis Sheridan | Synopsys |

CONEXXUS
*solve forward*

# 2019-2020 Conexxus Webinar Schedule

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

# NACS Show
# October 1-4, 2019
# Atlanta, GA

TECHEDGE

In partnership with CONEXXUS

Booth # 3755

## Conexxus thanks our 2019 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

wex

HUGHES An EchoStar Company

GILBARCO VEEDER-ROOT

Cybera

SECURITY INNOVATION

CONEXXUS
*solve forward*

# 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

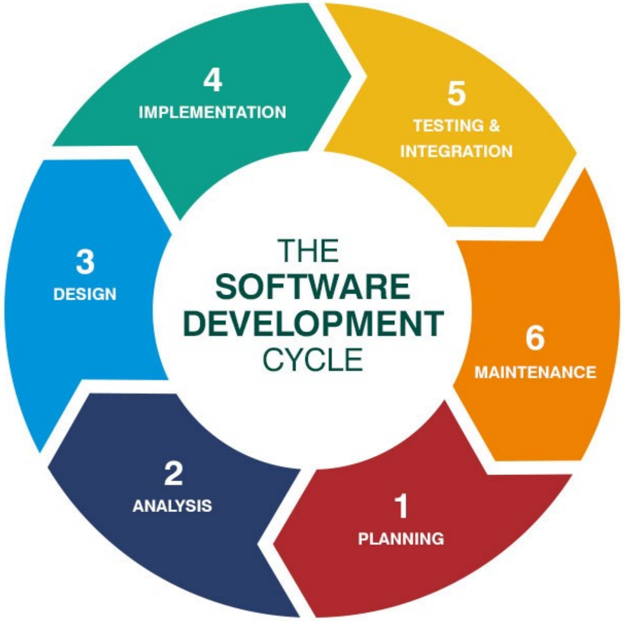
# Today’s Goal

- Raise awareness among builders and buyers of software
- Breadth not depth… but please interrupt me and ask questions ☺

# SECURE SDLC OVERVIEW

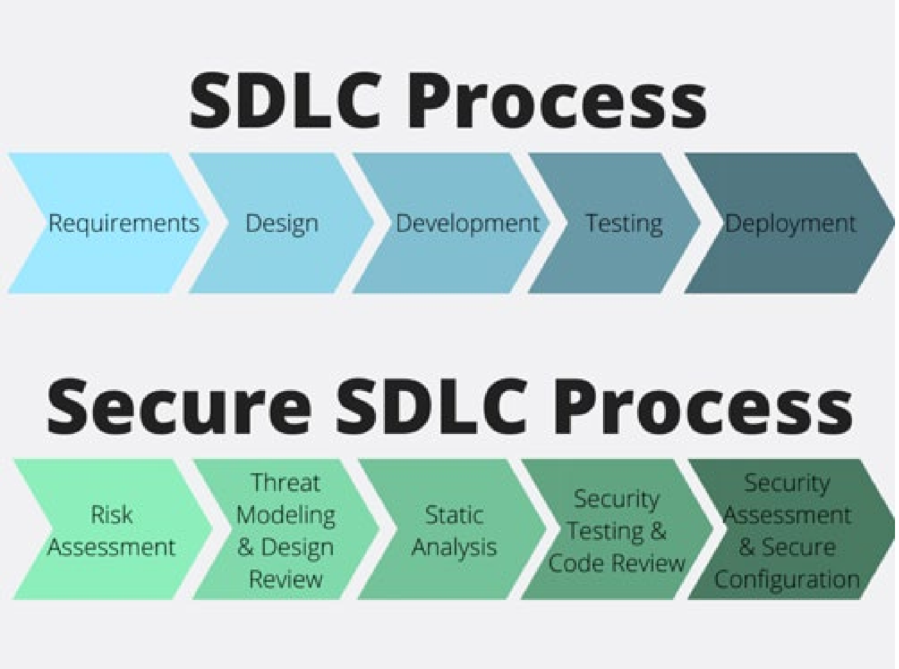
# Generic SDLC

- App idea
- Design solution
- Code it
- Test it
- Ship it



# Generic Secure SDLC

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



SDLC Process

Requirements → Design → Development → Testing → Deployment

Secure SDLC Process

Risk Assessment → Threat Modeling & Design Review → Static Analysis → Security Testing & Code Review → Security Assessment & Secure Configuration

# Security Methodology

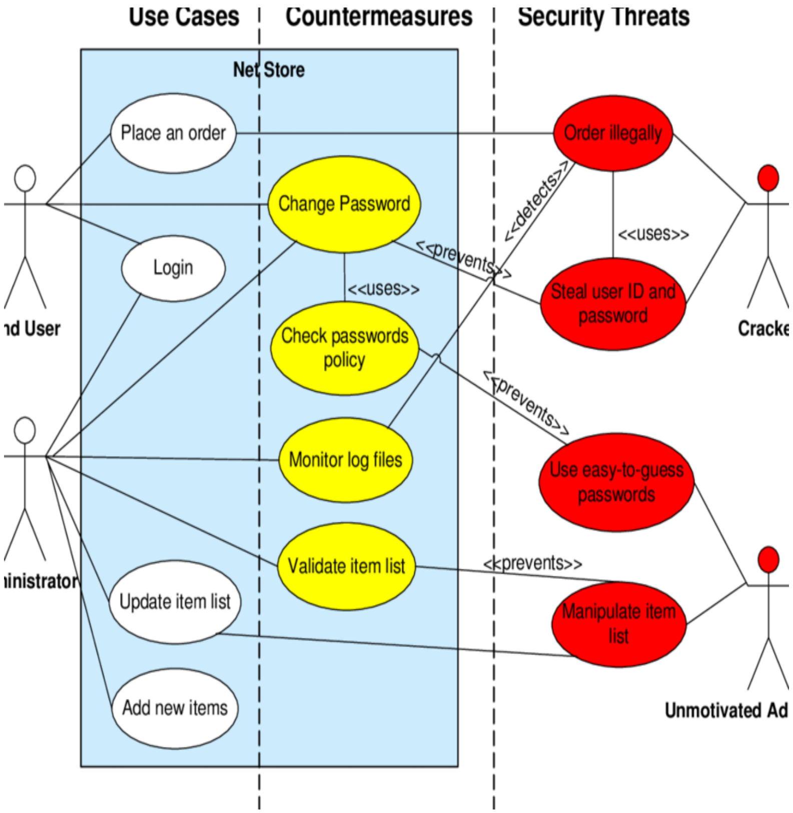
- “Think like an attacker” mindset
- Identify vulnerabilities and break assumptions
- Automated and manual approaches

Image credit: istockphoto.com/rscyther5

# SECURE SDLC ACTIVITIES

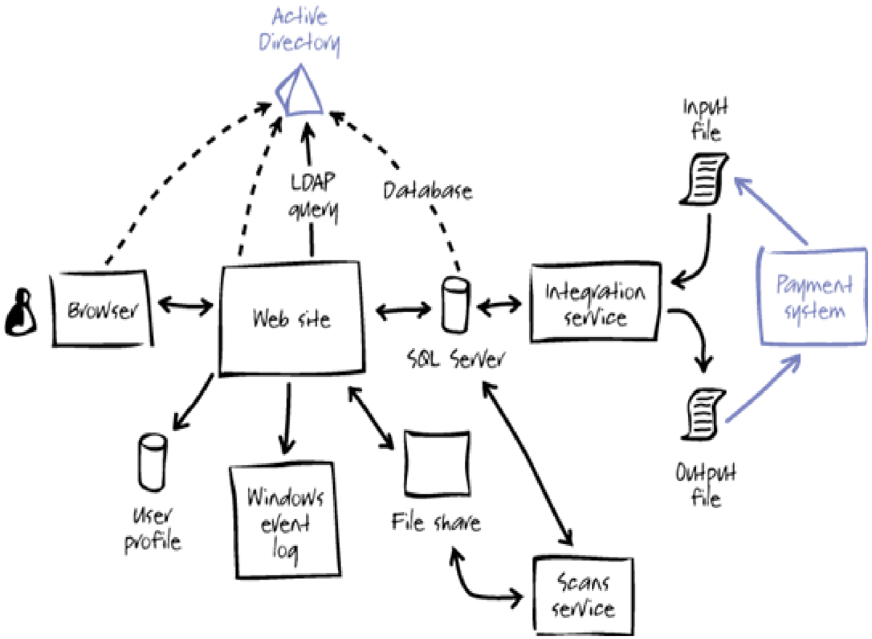
# Abuse Cases

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



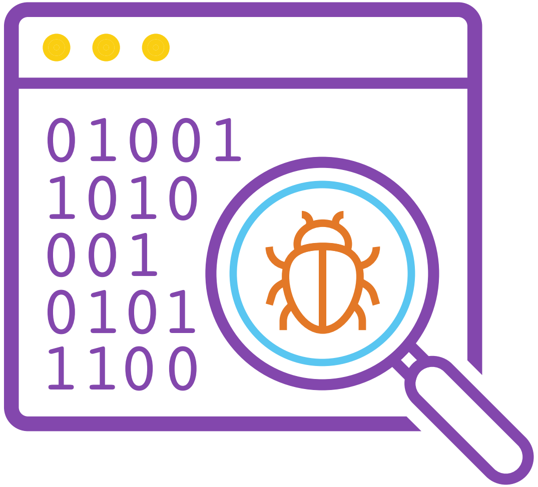
# Threat Modeling

- 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*

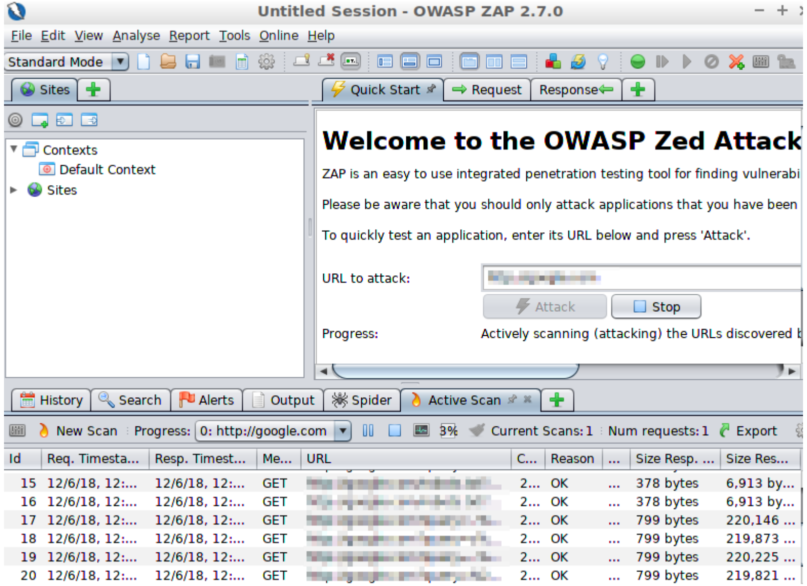


# Open Source Software

- 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



Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulnerabi

Please be aware that you should only attack applications that you have been

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: [redacted]

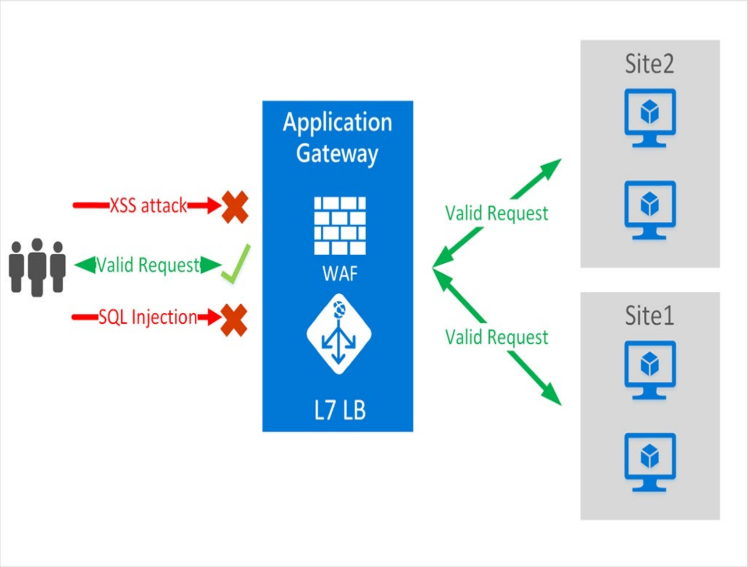
Progress: Actively scanning (attacking) the URLs discovered b

Progress: 0: http://google.com 3% Current Scans: 1 Num requests: 1

| Id | Req. Timesta... | Resp. Timest... | Me... | URL | C... | Reason | ... | Size Resp. ... | Size Res... |
|---|---|---|---|---|---|---|---|---|---|
| 15 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 378 bytes | 6,913 by... |
| 16 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 378 bytes | 6,913 by... |
| 17 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 799 bytes | 220,146 ... |
| 18 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 799 bytes | 219,873 ... |
| 19 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 799 bytes | 220,225 ... |
| 20 | 12/6/18, 12:... | 12/6/18, 12:... | GET | [redacted] | 2... | OK | ... | 799 bytes | 219,821 ... |

# Operational Security

- Web Application Firewall (WAF)
- Runtime Application Self-Protection (RASP)
- Code protections
- Bug bounty programs and responsible disclosure



CONEXXUS *solve forward*

# 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

CHARACTER

Indicate degree of each trait by A, B, C, D and E as in subjects.

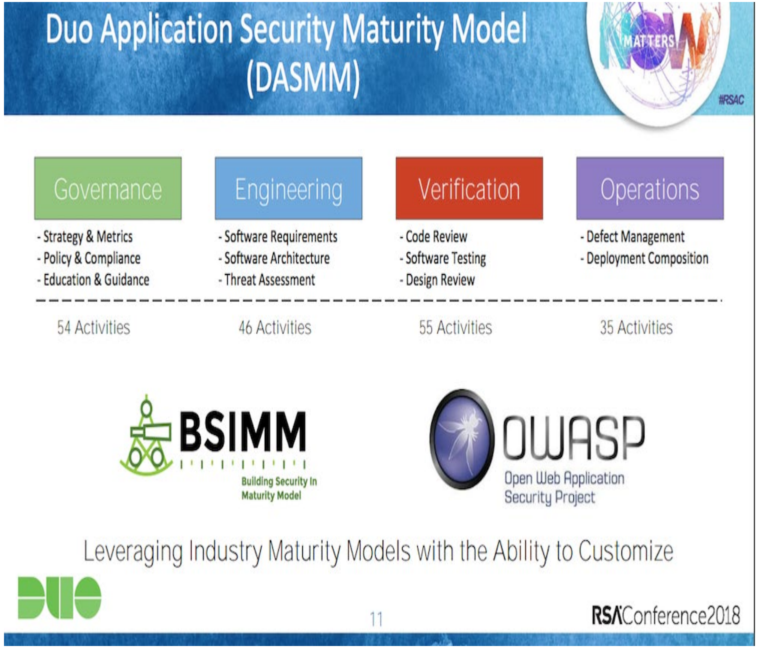
| TRAITS | 1st | 2nd | 3rd | 4th | 5th | 6th | 7th | 8th | 9th |
|---|---|---|---|---|---|---|---|---|---|
| Respect for School Property | A | A | A | A | A | A | | | |
| Obedience | A- | A | A | A | A | A | | | |
| Orderliness | B | A | A | A | A | A | | | |
| Promptness | A | A | A | A | A | A | | | |
| Courtesy | A | A | A | A | A | A | | | |
| Industry | A | A | A | A | A | A | | | |
| nce | B+ | A | A | A | A | A | | | |
| | A | A | A | A | A | A | | | |

89

90

# App Sec Program

- Company-defined approach to application security
- Balance security and speed to market
- Adapt to changes in development landscape



## Duo Application Security Maturity Model (DASMM)

| Governance | Engineering | Verification | Operations |
|---|---|---|---|
| - Strategy & Metrics<br>- Policy & Compliance<br>- Education & Guidance | - Software Requirements<br>- Software Architecture<br>- Threat Assessment | - Code Review<br>- Software Testing<br>- Design Review | - Defect Management<br>- Deployment Composition |
| 54 Activities | 46 Activities | 55 Activities | 35 Activities |

MATTERS NOW
#RSAC
BSIMM
Building Security In Maturity Model
OWASP
Open Web Application Security Project
DUO

Leveraging Industry Maturity Models with the Ability to Customize

11

RSAConference2018

Q
&
A

- 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.

# Images

- https://130e178e8f8ba617604b-8aedd782b7d22cfe0d1146da69a52436.ssl.cf1.rackcdn.com/application-security-four-key-steps-showcase_image-10-a-7778.jpg
- https://www.dignitasdigital.com/wp-content/uploads/2016/07/original-blog-image.png
- https://www.checkmarx.com/wp-content/uploads/2014/10/SDLC-Process.png
- https://i.ndtvimg.com/i/2017-09/cyber-crime-generic-istock_650x400_81504427706.jpg
- https://www.researchgate.net/profile/Mikko_Siponen/publication/221228994/figure/fig2/AS:667707808690183@1536205355641/An-example-of-an-extended-abuse-case-diagram-The-countermeasures-are-highlighted-in.png
- https://msdnshared.blob.core.windows.net/media/TNBlogsFS/BlogFileStorage/blogs_msdn/eugeniop/WindowsLiveWriter/WindowsAzureArchitectureGuidePart1Releas_F468/image_2.png
- https://www.synopsys.com/content/dam/synopsys/library/icons/icon-sig-coverity-static-analysis.svg.imgo.svg
- https://www.sigarch.org/wp-content/uploads/2017/12/AdobeStock_77494336-1080x675.jpeg

# Images

- http://www.sectechno.com/wp-content/uploads/2018/12/OWASP-ZAP.png
- 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:ANd9GcRSBRHYDb2u87Zqd4Avmtn23vvU_vAMKTZg6URgO2xMfMq0_pBI