Building a Scalable Security Engineering Team

Presenter:

Joe Basirico

SVP of Engineering

Security Innovation

CONEXXUS
solve forward

Agenda

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

Housekeeping

This webinar is being recorded and will be made available in approximately 30 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

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Jenny Bullard
Conexxus
jbullard@conexxus.org

Moderator

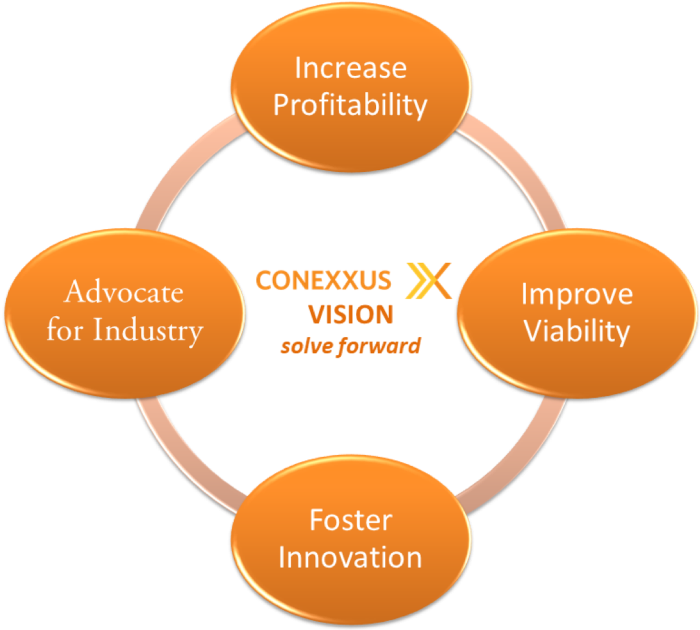
Jenny Bullard
Manager Membership Engagement
Conexxus
jbullard@conexxus.org

Speakers

Joe Basirico, SVP of Engineering, Security Innovation

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



2018 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
November 27, 2018	Fuel Fraud	Andrew McGloin Robert Alandt Sydney Green	Visa
November 29, 2018	Building a Scalable Security Engineering Team	Joe Basirico	Security Innovation
December 13, 2018	Chargebacks 101: The basics	Caleb Burke	CITGO Petroleum

2019 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
January 2019	Managed Detection and Reporting	Tom Callahan Mark Carl	ControlScan
February 2019	PCI DSS for Petro Merchants	Elizabeth Terry	PCI SSC
March 2019	Protecting Your Stores and Main Stores from Data Security & Ransomware Attacks	TBD	Acumera
April 2019	Don’t get Phished! Train Your Employees to Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
May 2019	Firewall compliance! The basics, the benefits, and the security	Simon Gamble	Mako Networks
June 2019	TBD	David Ezell Linda Toth	Verifone Conexxus

CONEXXUS
solve forward

Conexxus
Annual Conference

Loews Vanderbilt Hotel
Nashville, TN
April 28 - May 2, 2019

Conexxus thanks our 2018 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

GILBARCO VEEDER-ROOT

Cybera® Simplify Security and Networks

CONEXXUS solve forward

Building a Scalable Security Engineering Team

Presenter:

Joe Basirico

SVP of Engineering

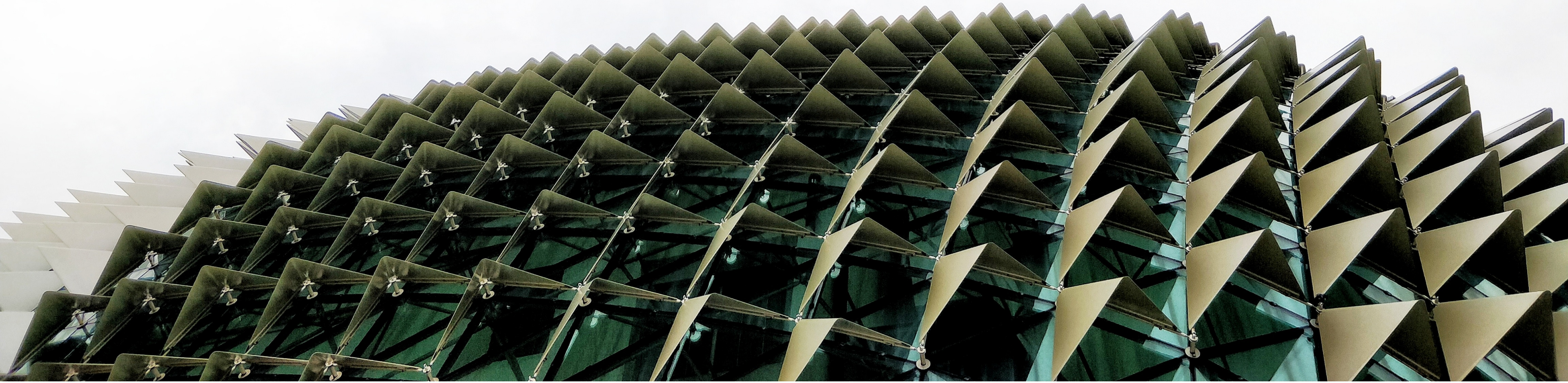
Security Innovation

Building a Scalable Security Engineering Team in 3 Easy Steps

1.Define Need

2.Build Culture

3.Build Team



Define Need

CONEXXUS
solve forward

Define Need

WHY DO YOU WANT A SECURITY TEAM?

WHAT ARE THE GOALS FOR THE ORGANIZATION?

WHAT DOES SUCCESS LOOK LIKE, *FOR YOU*?

Why?

- TO SHIP A SECURE PRODUCT
- SECURITY IS IMPORTANT TO OUR CUSTOMERS
- STAY OUT OF THE NEWS
- COMPLIANCE OR REGULATION
- A CORE ASPECT OF SOFTWARE QUALITY
- TO MANAGE VENDOR RISK

Define & Measure Success

- Spend time defining what success looks like
  - Trending fewer vulnerabilities
  - Spending less on Bug Bounties
  - Improved compliance / Reduced fines
  - Faster integration with external components
  - Improved relationships with vendors

- Prioritize your efforts – don't boil the ocean
  - Hire for your most important (or biggest gap) areas first

Set the framework

- Drastically increase the likelihood for success
- Give you resilience against changing corporate goals or budgets

Create & Track Metrics

If you can't measure it, you can't improve it.
- Peter Drucker

Make the metrics visible

- Surface them to the CISO/CEO to show value or areas for improvement

Fit to your organization

- What Microsoft or Amazon is doing probably isn't right for you
- One person can successful if enabled and their work is rightsized
- Align the team with the goals of the organization
  - Different teams may have different goals
  - Not all roles need to be Full Time

Goals
Improve Vendor Management/Relationship
Enable Security Leadership
Become compliant
Security Leadership during integration

SET UP FOR SUCCESS

Clearly Define Roles and Responsibilities

Enable

- Knowledge Base
- Q&A
- Guidance
- Education
- Tooling
- Compliance review
- Integration help

Enforce

- Assessment
- Vulnerability tracking
- Security Gates
- Block Ship/Deploy/Integration

Empower to create a healthy team

Problems stem from resource scarcity

Budget

Time

Promotion opportunities

Me vs. you

Us vs. them

Keystones of a healthy team

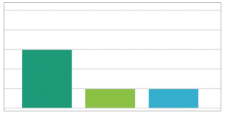
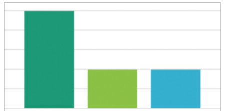
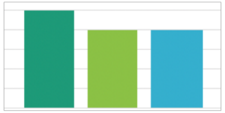
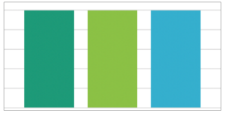
Communication (internal and external)

Focus on Mission, Objectives, Results

Strong Leadership

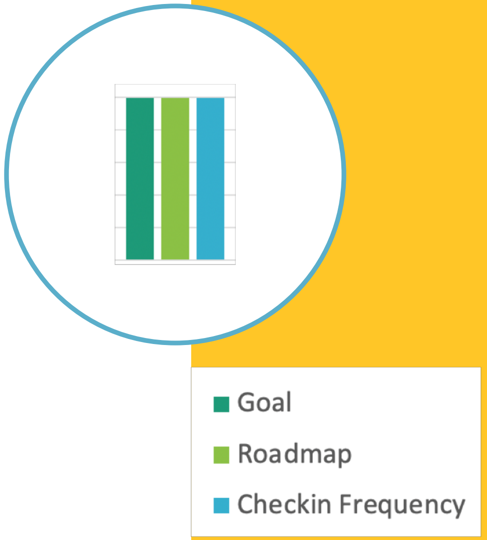
Diverse

Support vs. Direction

Role	Goal	Roadmap	Check-ins	
Principal	Employee Created	Employee Created	Beginning/Middle/End	
Senior	Clear	Rough outline	Beginning/Middle/End	
Engineer	Clear	Detailed	Periodic	
New Hire	Clear	Detailed	Frequent	

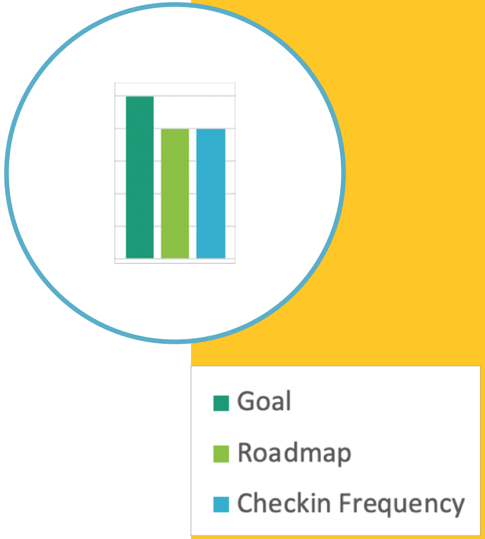
New Hire

- Needs clear support and direction
- Unmatched opportunity to instill culture
- Time spent here will pay dividends later
- Support, don’t micro-manage



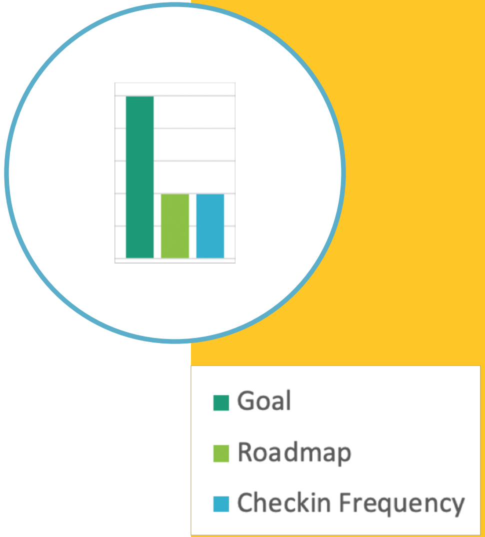
Engineer

- Can carry out most tasks autonomously
- Needs fewer check-ins and a less detailed roadmap
- Starts to think about leading, improving, challenging



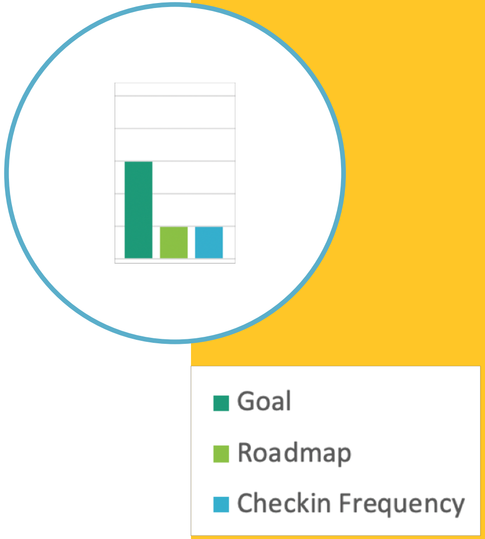
Senior Engineer

- Leads projects
- Improves methodology, tooling
- Trains others
- Communicates clearly
- Devises their own roadmap to a goal
- Is self starting, guiding, organized

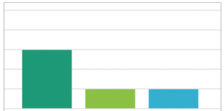
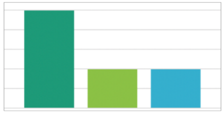
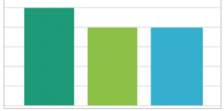
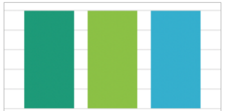


Principal Engineer

- Sets goals collaboratively
- Leads the team explicitly or by example
- Collaborates with manager to achieve goals
- Check-ins are infrequent



Pre-promote to test readiness and challenge

Role	Goal	Roadmap	Check-ins	
Principal	Employee Created	Employee Created	Beginning/Middle/End	
Senior	Clear	Rough outline	Beginning/Middle/End	
Engineer	Clear	Detailed	Periodic	
New Hire	Clear	Detailed	Frequent	

CONEXXUS
solve forward

Security Teams are Different

CULTURE

Autonomy Mastery Purpose

Understand Motivation/Incentives

“The most damaging phrase in the language is ‘we’ve always done it this way!’”
— Grace Hopper

Autonomy
Control over one’s own goals

Mastery
Ability to build skills and become a master

Purpose
Work in service to a larger goal

Understand Motivation/Incentives

Autonomy

Control over one’s own goals

- Ability to pursue unknowns through research
- Self directed professional development time
- Ownership over tooling, methodology, reporting, to improve

Mastery

Ability to build skills and become a master

Purpose

Work in service to a larger goal

Understand Motivation/Incentives

Autonomy

Control over one’s own goals

Mastery

Ability to build skills and become a master

- Time to improve
- Buffer time between projects
- Conferences attendance (self selected, links to autonomy)
- Company paid certifications, trainings, etc.

Purpose

Work in service to a larger goal

Understand Motivation/Incentives

Autonomy
Control over one’s own goals

Mastery
Ability to build skills and become a master

Purpose
Work in service to a larger goal

- Code of Conduct
- Responsible Disclosure policy
- Individual goals link to company goals
- Time to dedicate to OSS/public github pages

HIRING AND RECRUITING

"Our people are our most valuable asset"

Market that!

Market Your Culture

Your people and your culture will attract more of the same

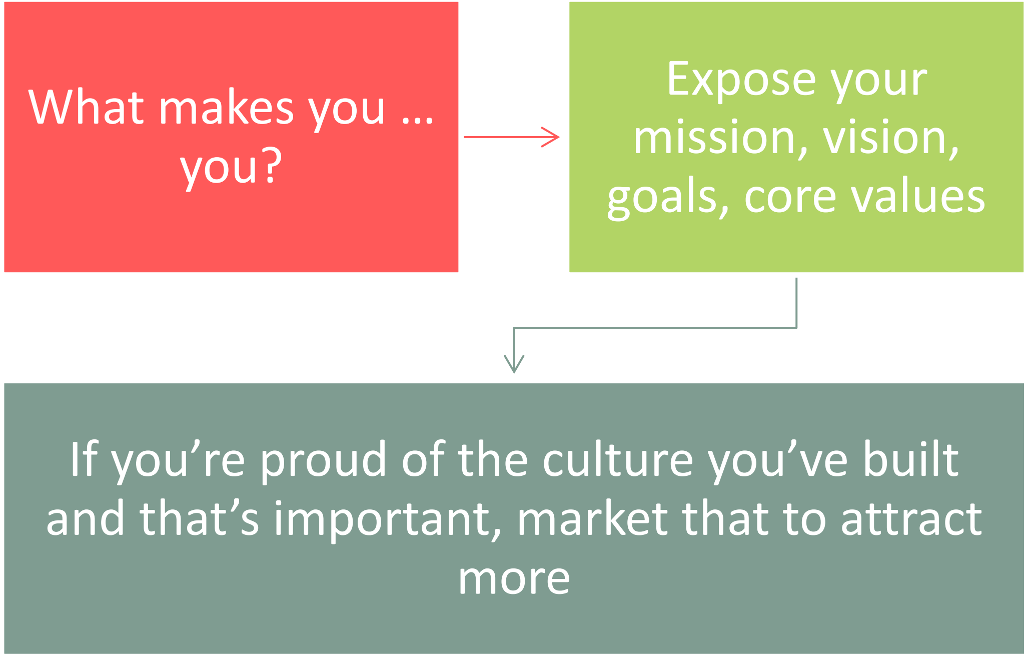
Emulate the culture you want to have

Attend and Speak at conferences

Identify research conferences vs. industry tradeshows

Maintain and contribute to OSS

Your culture will attract more



What makes you … you?

Expose your mission, vision, goals, core values

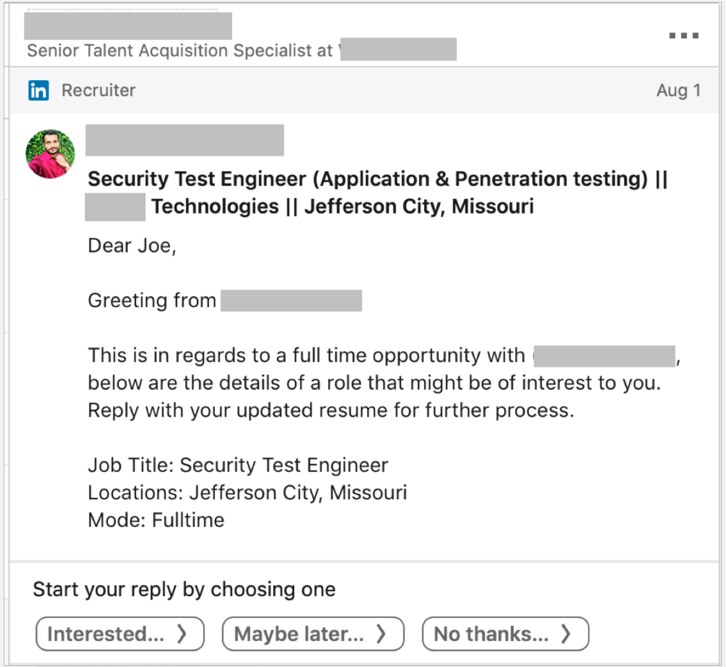
If you’re proud of the culture you’ve built and that’s important, market that to attract more

Emulate what you want

- Have you seen an exceptional team?
  - What makes them tick?
  - What attracts people to work there?
  - Improve and adapt what you see to fit your culture

“Good artists copy. Great artists steal.”

Recruiting



[redacted]

Senior Talent Acquisition Specialist at [redacted]

[redacted]

Security Test Engineer (Application & Penetration testing) || [redacted] Technologies || Jefferson City, Missouri

Dear Joe,

Greeting from [redacted]

This is in regards to a full time opportunity with [redacted], below are the details of a role that might be of interest to you. Reply with your updated resume for further process.

Job Title: Security Test Engineer
Locations: Jefferson City, Missouri
Mode: Fulltime

Start your reply by choosing one

- Most great engineers are already happy with their current jobs
  - Customized recruiting messages from interesting people
  - Impersonal recruiting tactics don’t work
- Cast a wide net, filter with a custom challenge site
  - Not just busy work
  - Something
    - Interesting
    - Challenging
    - Worth doing
    - Aligns with your industry and team

Training

- Consider starting a “feeder program”
- Hire people with great potential
- Link them to a great training program

Pros

- Hiring pool is larger
- Training is customized to you
- Can be less expensive initially

Cons

- Ramp-up time
- Investment in training program
- Lack of existing culture, process, methodology

Onboarding

- New hires need the most support, but beyond basic orientation don’t get enough
- Think of this as the opportunity to not only get accounts set up, but also to instill
  - Culture
  - Expectations
  - Communication
  - Methodology
  - Reporting
  - Code of Conduct

Summary

Define need, and success

Give clear direction, goals, and support

Set a Mission & Vision for the team

Set up for success

Clearly define roles and responsibilities

Empower a healthy team

Build Culture

Understand your engineers and their incentives

Autonomy, Mastery, Purpose

Build Team

Market your culture

Recruit in unique places

Create a training and onboarding process as unique as you are

Questions?

SECURITY
INNOVATION

Joe Basirico
SVP of Engineering
jbasirico@securityinnovation.com
(206) 508-1001

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