



The Tactical Application Security Program: Getting Stuff Done

Cory Scott & David Cintz, LinkedIn

@cory_scott | @David_C_Z

Who Are We?



Cory Scott

Director, House Security @ LinkedIn

Previously at Matasano Security,
ABN AMRO/RBS, @stake

Likes: Cat pictures

Dislikes: Improperly chilled beer



David Cintz

Senior Technical Program Manager,
House Security @ LinkedIn

Previously at Black Hat, Zynga,
Chevron

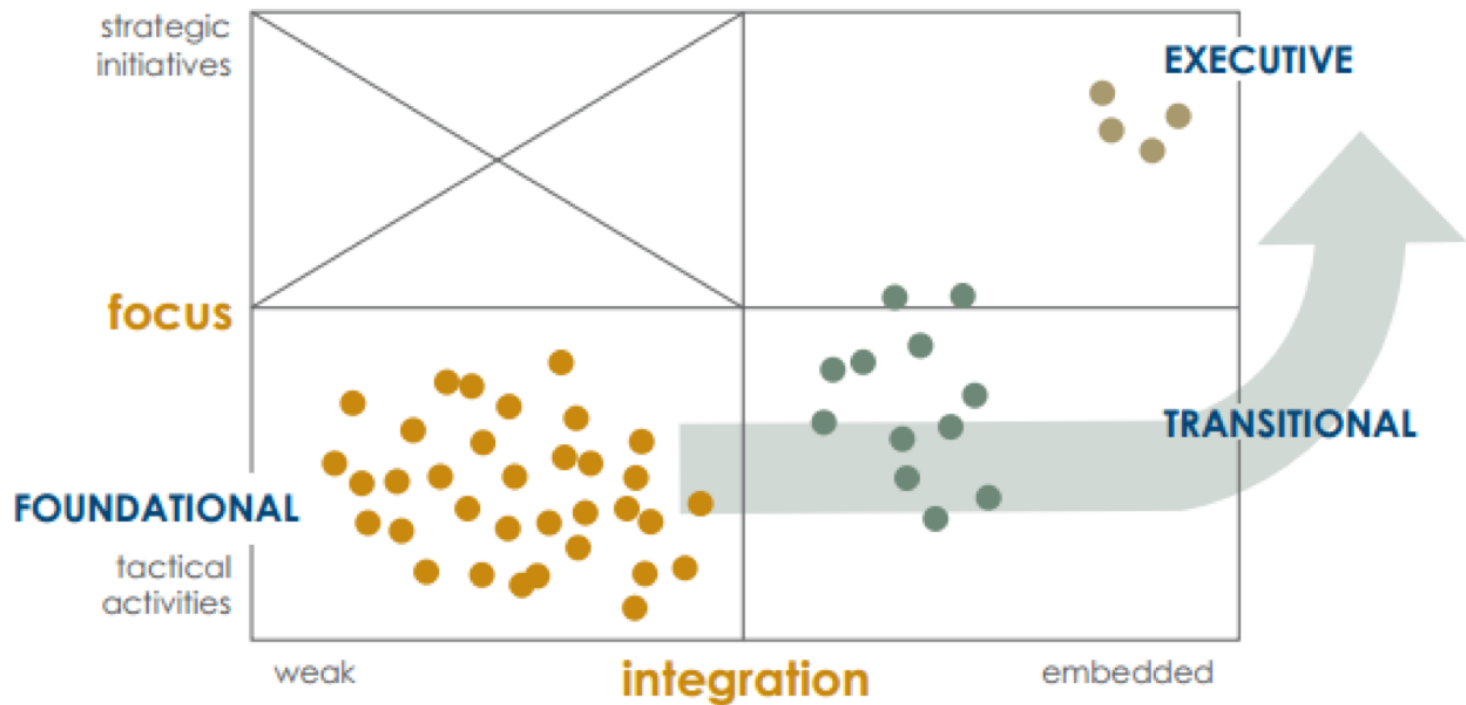
Likes: Flying planes

Dislikes: Automatic towel dispensers

Agenda

- **Elements of a Tactical Security Program**
- Application Assessment
- Application Incident Response
- Bug Bounty Programs

The Strategic-Executive Siren Song



How To “Strategically” Fail

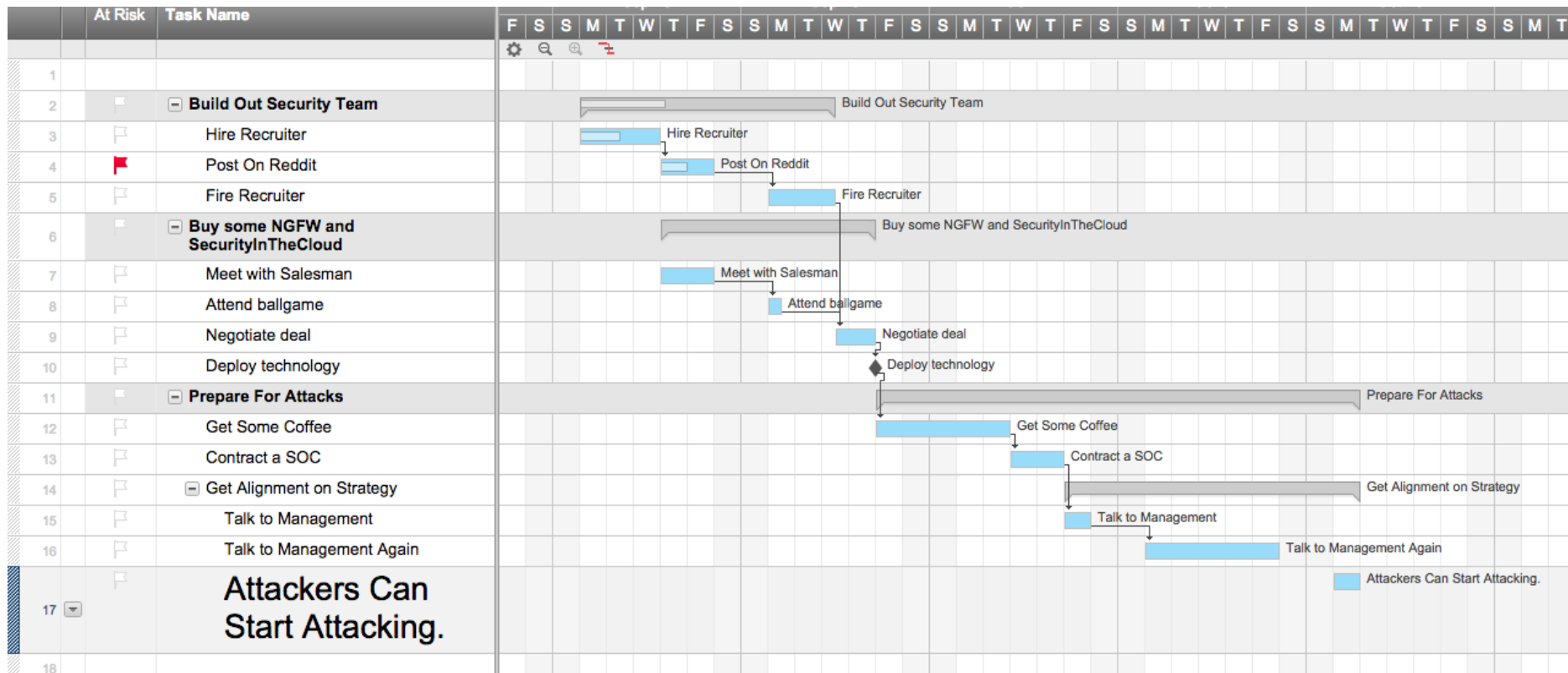
- Application security doesn’t survive strategically
- Perpetually deferred reward vs immediate value
- A primer on management psychology
- Why your non-security peers love to hear the word strategy

This is Your Security Life and You're Ending It With One Failed Strategy at a Time

It may be common to think of technological tools and organizational policies and procedures when dealing with information security. However, a strategy for enterprise security should be developed first. This strategy should be based upon a thorough analysis of the threats faced by the enterprise, the potential impact (legal, financial, and reputational) of those threats, and all the resources available to address the threats. Such a strategic approach to security should help enterprises find the most efficient ways to mitigate security risks. An enterprise may find that issues that appear to be vendor and workforce management problems at first glance can be better mitigated through access management.

<http://www.infolawgroup.com/2014/02/articles/information-security/information-security-strategy-a-lesson-from-the-target-breach/>

You Can't Defeat Today's Attacks With A Gantt Chart



Elements of A Tactical Security Program

- Lightweight and iterative
- Can demonstrably reduce vulnerability or risk for each action taken
- Focuses on operational excellence, less on being a dreamer/architect of the “perfect solution” or getting 100% buyin across the organization
- Makes others move rather than wait

Start small,
experiment, pivot,
and communicate.

Every action
should have an
explicit value that
can be explained.

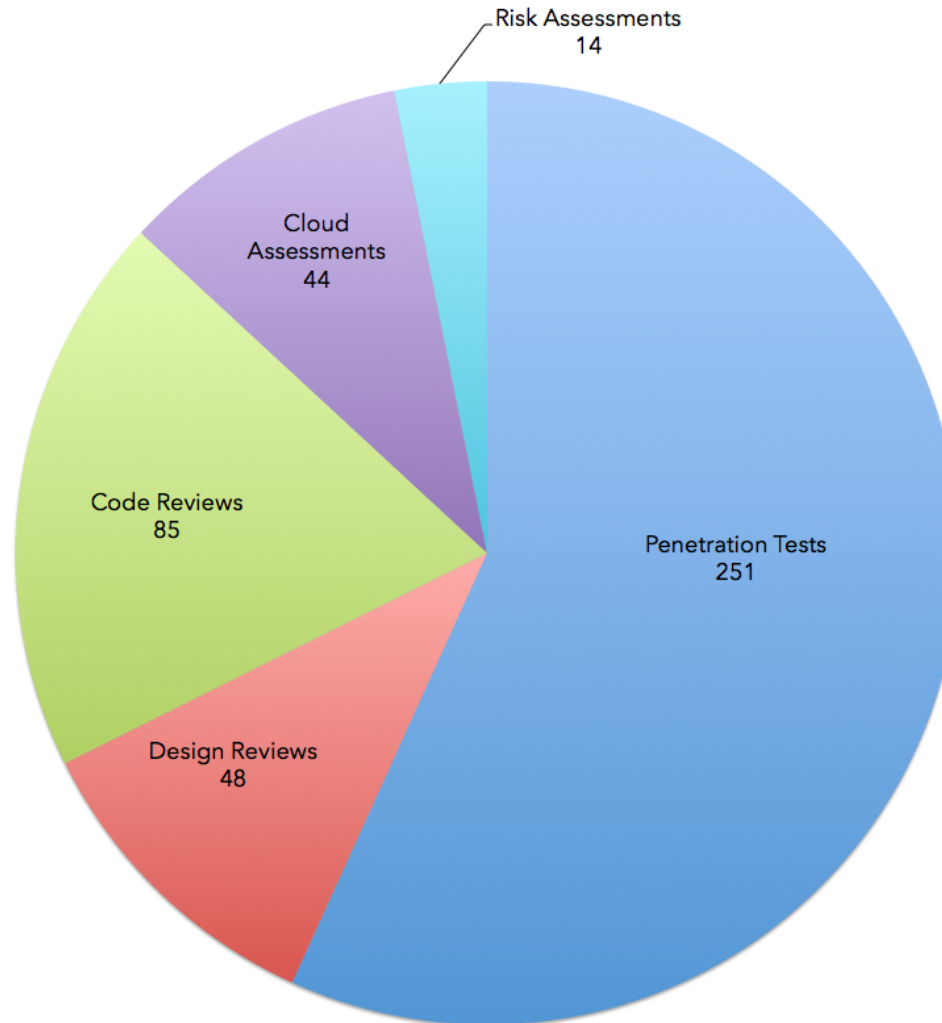
Lead with your
ability to execute
first.

Bring others along
- don't try to solve
things by yourself.

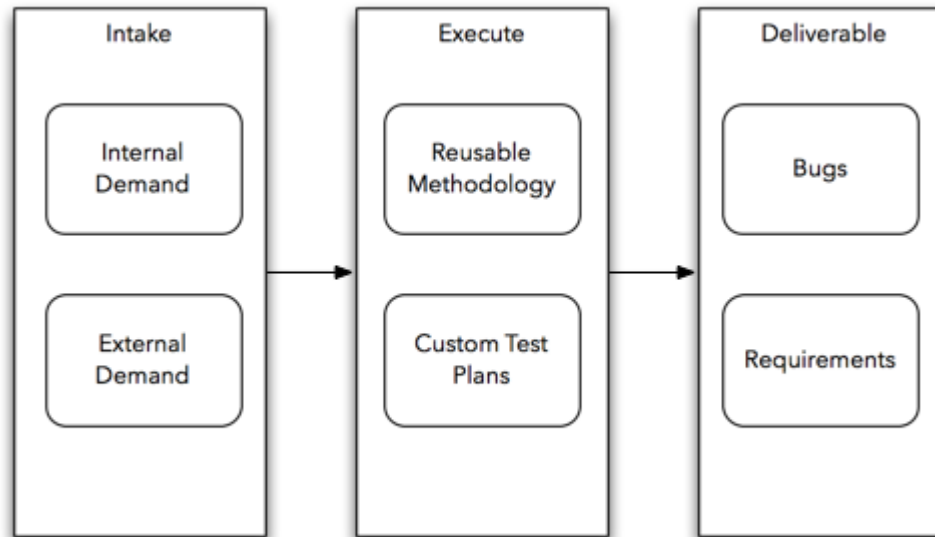
Agenda

- Elements of a Tactical Security Program
- **Application Assessment**
- Application Incident Response
- Bug Bounty Programs

A Year Of Assessments At LinkedIn



Assessments have a Flow



Evaluate your assessment activity like a flow. Where are you strongest? What needs improvement?

Tactical Assessment Principles

1. Be easy to find and quick to engage.
2. Be flexible on documentation & preparation.
3. Give clear guidance that has a reasonable likelihood of being executed.
4. Jointly engage with legal, customer support, and other groups in engineering for leverage.
5. Be passionate yet practical; don't pass judgment or punish.

Office Hours

Time (PM PST)	Product	Product Description (REQUIRED) ~Please provide wiki links, if available~	Requestor Name (example: Fred Flintstone)	Discussion Outcome ===== ! HSEC USE ONLY ! * To be completed by HOUSE SECURITY team DURING the discussion *	Assessment Type (example: Pen Test Design Review Code Review) ===== ! HSEC USE ONLY !	PWN Ticket # ===== ! HSEC USE ONLY !	PWN Ticket ===== ! HSEC USE ONLY !	House Security Attendee
3:00	Endorse-a-lot	More endorsements	Bob	Recommend design review.	Design Review	PWN-1234	Create JIRA Tick	Homer
3:30	CatCrowd	Migrate cat pictures to a crowdsourced model	Roger	Needs pentest	Pen Test	PWN-1235	Create JIRA Tick	Homer
4:00	Operation Lockdown	Influencer post security controls	Carl	Design looks good. No further review needed.	None	N/A	Create JIRA Tick	Marge
4:30	Much payment	Support dogecoin for checkout flow	Lennie	Need some sample coins and some code review.	Code Review	PWN-2383	Create JIRA Tick	Marge

Assessment Tactics

- Build a service catalog
- Document your methodology, define game-overs, don't be afraid to trim
- Navigating the wilderness of existential assessment questions

Generating Assessment Demand: Stuff That Matters

- Be a part of product launch flow
 - Look for the business decision points where projects are approved
 - Insert yourself into the design process post-approval
 - Look for opportunities to contribute security guidance outside of just pentesting or code review
 - Whitepapers
 - Third-party assessments
 - Communications & product marketing
 - Abuse detection and monitoring
- Watch for changes in staging and production
- Befriend the gatekeepers
 - Domain registration
 - DNS changes
 - Traffic & front-end routes

Pitfalls

- Unwanted and uninteresting reviews
- Standards and self-certification
- Missing the big picture



Lead, Follow, or Get Out Of The Way

- In an external consultancy, your goal is exclusive: client satisfaction.
- In an internal security team, you must balance:
 - Developer / Business Owner Satisfaction
 - Overarching company governance and security
 - Precedent-setting behavior
 - Customer and member safety
- The case of LinkedIn Intro

Agenda


- Elements of a Tactical Security Program
- Application Assessment
- **Application Incident Response**
- Bug Bounty Programs

Handling Outside Reports


- We receive reports via:
 - Security alias - security@linkedin.com
 - Social media
 - Customer service tickets
 - Executive escalations
- On call pentester to handle incoming reports
- SLA
 - 4 hours to triage and respond
 - 8 hours weekends and nights - only handle criticals
- Responsibilities of on call
 - Triage
 - Respond
 - File tickets
- Basic human response
 - Acknowledge report
 - Investigating issue

Case Study - Changing Faces

- We received the report after hours
- Soon discovered the report was not the original
 - Found the original as a YouTube video
- Responded and implemented stop-gap solution within the hour
- Demo...

 PREMIUM Advanced 17 7

Home Profile Connections Jobs Interests Business Solutions Go to Recruiter



Tony Trummer 1st PREMIUM
Staff Engineer, Information Security at LinkedIn
San Francisco Bay Area | Information Technology and Services
Previous LinkedIn, Warner Bros. Entertainment Group of Companies, ReachLocal
Education University of Arizona
[Send a message](#) 345 connections


Does Tony have these skills or expertise?


Security x Penetration Testing x Firewalls x VPN x

Information Security x


[Endorse](#) [Skip](#) What is this?


Background


 Summary
Constantly trying to find the bug before the bad guys do.

 Experience
Staff Engineer, Information Security
LinkedIn
September 2014 – Present (11 months) | Mountain View, CA
1 course


In Common with Tony





 PREMIUM Advanced 17 7

Home Profile Connections Jobs Interests Business Solutions Go to Recruiter



🐼 Tony Trummer 🐼 1st PREMIUM
Staff Engineer, Information Security at LinkedIn
San Francisco Bay Area | Information Technology and Services
Previous LinkedIn, Warner Bros. Entertainment Group of Companies, ReachLocal
Education University of Arizona
[Send a message](#) 345 connections


Does 🐼 Tony have these skills or expertise?


Security x Penetration Testing x Firewalls x VPN x

Information Security x


[Endorse](#) [Skip](#) What is this?


Background


 Summary
Constantly trying to find the bug before the bad guys do.

 Experience
Staff Engineer, Information Security
LinkedIn
September 2014 – Present (11 months) | Mountain View, CA
1 course


In Common with 🐼 Tony





 PREMIUM Advanced 17 7

Home Profile Connections Jobs Interests Business Solutions Go to Recruiter



Tony Trummer 1st PREMIUM
Staff Engineer, Information Security at LinkedIn
San Francisco Bay Area | Information Technology and Services
Previous Education
LinkedIn, Warner Bros. Entertainment Group of Companies, ReachLocal
University of Arizona
[Send a message](#) 345 connections


Does Tony have these skills or expertise?


Security x Penetration Testing x Firewalls x VPN x

Information Security x

[Endorse](#) [Skip](#) What is this?

Background

 Summary
Constantly trying to find the bug before the bad guys do.

 Experience
Staff Engineer, Information Security
LinkedIn
September 2014 – Present (11 months) | Mountain View, CA
1 course

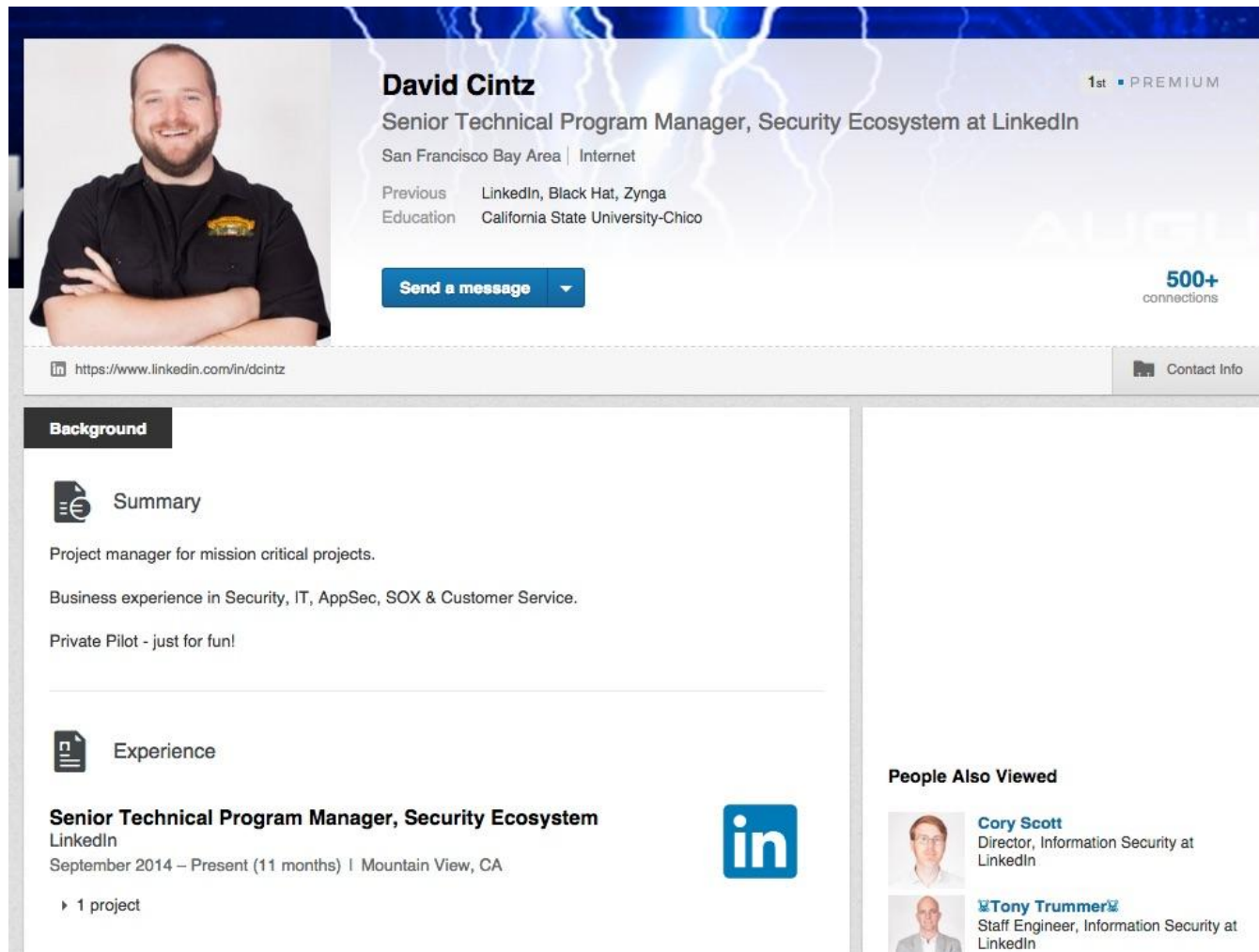
In Common with Tony

1 Skill or Expertise
3 Groups
1 Company
1 Location

Case Study - Changing Faces Continued...

- Report came in after hours
 - Triaged and responded in about an hour
- What makes this a critical?
 - Bug Classification Table
 - Contains specific examples
 - Provides clear guidance
 - Has established Service Level Agreements (SLAs)
- LinkedIn is an online service company
 - We can push code quickly
 - Sometimes not quick enough
 - Forced to use stop-gap solutions

Cleanup After the Incident



The image is a screenshot of a LinkedIn profile for David Cintz. The profile header shows a photo of a man with a beard and arms crossed, the name 'David Cintz', and his title 'Senior Technical Program Manager, Security Ecosystem at LinkedIn'. It also lists his location as 'San Francisco Bay Area | Internet', previous employers as 'LinkedIn, Black Hat, Zynga', and education at 'California State University-Chico'. A 'Send a message' button and '500+ connections' are visible. Below the header, the 'Background' section is active, showing a 'Summary' with text about mission critical projects, security experience, and being a private pilot. The 'Experience' section shows his current role at LinkedIn from September 2014 to present. On the right, a 'People Also Viewed' section lists Cory Scott and Tony Trummer.

David Cintz 1st • PREMIUM
Senior Technical Program Manager, Security Ecosystem at LinkedIn
San Francisco Bay Area | Internet
Previous LinkedIn, Black Hat, Zynga
Education California State University-Chico
Send a message
500+ connections
https://www.linkedin.com/in/dcintz Contact Info

Background

Summary
Project manager for mission critical projects.
Business experience in Security, IT, AppSec, SOX & Customer Service.
Private Pilot - just for fun!

Experience
Senior Technical Program Manager, Security Ecosystem
LinkedIn
September 2014 – Present (11 months) | Mountain View, CA
1 project

People Also Viewed
Cory Scott
Director, Information Security at LinkedIn
Tony Trummer
Staff Engineer, Information Security at LinkedIn

Determining Scope of Impact

- Do NOT wait until the incident is over
- Start research in parallel
- Application response team needs access to log data.

What we use at LinkedIn:

- Elasticsearch
- HDFS / Hadoop / Hive
- Dedicated data science team is great, though not a necessity

Don't wait until you are in the midst of an incident to find out that you don't have proper logs or the IP address being captured of your attacker is that of your own CDN.

Case Study

- Externally reported through our bug bounty program
- Demonstrated that he could delete any embedded video from any SlideShare presentation
- On-call engineer discovered that he could add a video to any SlideShare presentation
 - Not part of the original report
 - Discovered during triaging bug
- Impact is clear, easy to explain why it's a critical
 - Not all bugs are this straightforward

Bug Classifications and Why We Built It

- We/You are the face of security
- We have to convince people to fix things
 - Resulting in being labeled _____ when we stand our ground
 - ‘grumpy’
 - ‘argumentative’
 - ‘jerk’
- Teams will game the system and argue
 - Impact
 - Complexity
 - Accessibility
 - Wormability
 - “It has existed like that for years”
- CVSS approach will also lead to arguments (*aka “discussions”*)

Sample Bug Classification Table

Severity	Remediation Time (100% Production)
Critical	Same Day - All Hands On Deck
High	5 business days
Medium	15 business days
Low	30 business days

Bug Class	Asset Impacted	Severity
Credential leakage	Any user-provided passwords, OAuth tokens, and authentication cookies	Critical
API token leakage	OAuth tokens	Critical
SQL / ORM injection	*.example.com,	Critical
Cross-Site Scripting - Stored	*.example.com	Critical
Remote Code Execution	Any corporate Internet-exposed asset	Critical
Cross-Site Request Forgery (excluding logout)	www.example.com	High
Bypass of abuse controls	www.example.com ,	High
Insecure transmission of sensitive member data over the Internet	*.example.com	High
Clickjacking / Framing – secured settings, inbox and invites	www.example.com	High
Mixed-Content Issues	*.example.com	Medium
Open redirect without signature	*.example.com	Medium
Server or application information disclosure	www.example.com , api.example.com	Low

Importance of Communication During an Incident

- Incident success or failure is judged by others in your company
- Coordination and communication are key
 - Many teams are involved typically
 - Need to get updates to a centralized point
 - Communication must flow in all directions - including up
- Management should never hear about an incident second hand
- Provide official updates from a dedicated person
 - Summary of issue
 - Potential impact
 - Next steps
 - Planned remediation (if available)

Emails to the management should be sent on a regular basis. If you do not have someone like me to do this, that's ok too; just set the expectation for when the next update will happen.

Communication Email Template

Friday, January 23, 2015 at 4:57:20 PM Pacific Standard Time

Subject: Critical Security Issue - Brief Summary - MARK IMPORTANT

Date: Friday, January 23, 2015 at 4:56:58 PM Pacific Standard Time

From: David Cintz

****Headline – 1 line summary****

Paragraph 1 : Issue, explain what the issue is, how it was discovered, where it was discovered and impact to business.

Paragraph 2: Actions taken thus far, include who has been contacted, what are next steps, is there reason to believe malicious exploitation?

Paragraph 3:

1 line Summary of issue (from JIRA ticket)

URL to PWN Ticket

Issue Severity: Critical – All hands on deck

Paragraph 4: Thank you to team(s)

Paragraph 5: Boilerplate – copy/paste

Please note because this is a critical severity issue, the standard process is to send out a notification email (this email) with the details of the issue and the status to management. This email is not an escalation, but rather giving management visibility into security issues across the company as they have requested. I will be sending updates as they become available.

Using Playbooks

- Developing a standard playbook is a must
- Will provide guidance and framework
- Living document
- Not 100 pages
 - Must be easy to use
 - No one will update
 - No one will read
 - No one will use
- Share playbook / be transparent with partner teams
 - Publish playbook
 - Tell them what is going to happen

Reducing the Threat Surface

- Be consultative: explore potential short-term and long-term fixes
- For application vulnerabilities
 - Disable functionality through configuration or A/B test control
 - Hint: encourage the development of new functionality and bug fixes behind A/B testing
 - Block - “When only HTTP error codes will do”
 - Reverse proxy for endpoints
 - Specialized filters for request body filtering
 - Monitor for abuse

While you can allow the “long term fix” discussion to happen and is completely acceptable, focus has to maintain on mitigating the threat now.

Agenda

- Elements of a Tactical Security Program
- Application Assessment
- Application Incident Response
- **Bug Bounty Programs**

Case Study

- External researcher published a blog post about Intro product
 - No disclosure to LinkedIn prior to post
 - No attempt to reach out to LinkedIn
- We opted to talk with the author
 - Did NOT involve legal
 - Reached out with a simple invite to chat
 - Goal was to work collaboratively
- This resulted in positive outcome
 - Fixed bug same day
 - Researcher/Author was happy
 - Follow up blog post was super positive
- Focus on building relationships with researchers
 - Communicate and be transparent (as much as possible)
 - Understand the motivation of the researchers

This is not and should not be an adversarial relationship - it's completely the contrary. This change in attitude on both sides means that both parties win.

Public Bug Bounties Today

- Main motivations for companies to build programs
 - Receive quality reports
 - Establish good relationship with security community
 - Stay out of negative light
 - Good use of money & resources
- In contrary these programs have fostered an influx of false and bad reports
 - Beg bounty hunters
- Signal to noise ratio constantly degrading
 - Companies forced to use dedicated resources
 - Engage consultancies
 - Use platform vendor to sift through the chaff

How We Adopted Our Current Program

- Previously, a vast majority of reports to LinkedIn were not actionable or meaningful
- Smaller group of researchers emerged
 - Provided quality bugs
 - Provided quality write-ups
 - Genuinely interested improving security
 - Fun to work with and engaging
- They wanted to work with us - we liked working with them
 - Why not reward them?
 - This was the spirit of the original programs
- Allows us to grow our relationships with researchers
 - Receive more meaningful reports
 - Give more meaningful responses
 - More time to focus on analysis and proper fixes

LinkedIn Program Now

- Launched LinkedIn private program October 2014
 - Paid out over \$65,000 bounties
 - Received more than 65 actionable reports
 - Signal to noise ratio 7:3
- We have seen significant reduction in authorization-related issues
 - Has helped us identify bugs in older code that did not get same level of attention
 - Influx of great reports - rewarding for certain types of research that show creativity or persistence
- Less “gamesmanship” of program - Public programs incentivise Junk reports
 - Researchers trying to beat the clock - submit as soon as possible
 - Incentivise low hanging fruit / best practice sighting
 - No incentive for in-depth analysis or write-ups
 - Flat out copying from other programs (even forgetting to change company name)

What Do These Ratios Really Mean to Me?!

- Signal to Noise ratios don't mean much, unless you do the math
- Industry average is approximately 1:20
- Average time breakdown
 - Triage report: 30 minutes
 - Communications / file bug: 10 minutes
 - Total time per report: 40 minutes
- Hypothetical company receives 21 bugs a week
- Resulting in 17.5 hours of work per week
- Devil's advocate - reduce by 25% for automation
 - Results in 13 hours per week
- All that work for 1 quality bug

Wrapping Up

- Tactical approaches to application security should be embraced
- Treat your assessment program like a consultancy
- Application incident response may be the most important thing to get right
- Focus on treating external vulnerability researchers right first, then consider bounty programs