black hat®
ASIA 2016

The Tactical Application Security Program: Getting Stuff Done

Cory Scott & David Cintz, LinkedIn
@cory_scott | @David_C_Z

UBM

Cory Scott

Sr. Director, House Security @ LinkedIn

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

Likes: Cat pictures

Dislikes: Improperly chilled beer

David Cintz

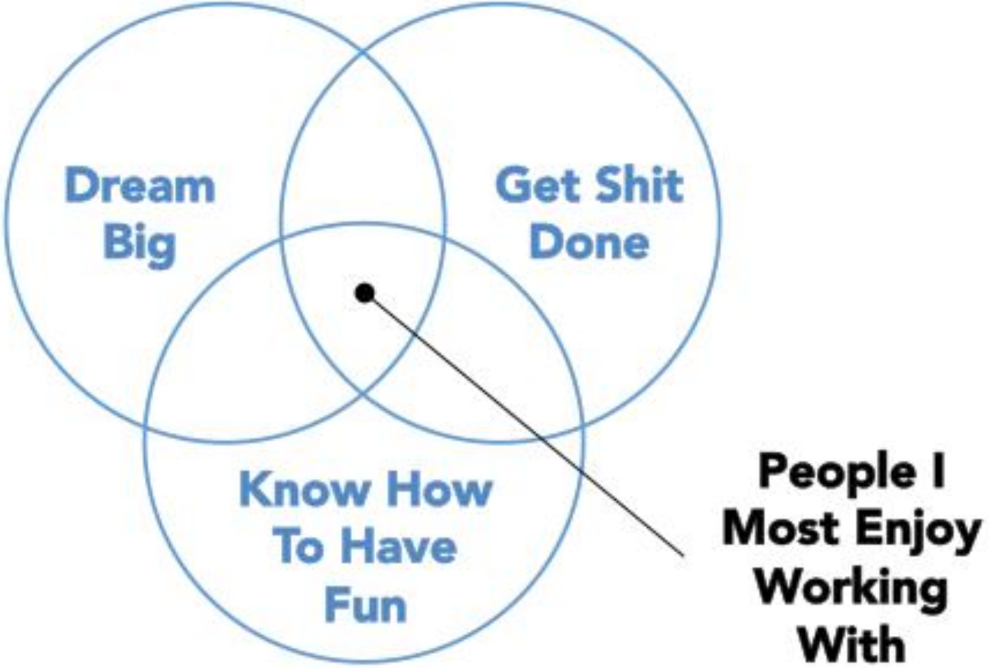
Staff Security Program Manager,
House Security @ LinkedIn

Previously at Black Hat, Zynga,
Chevron

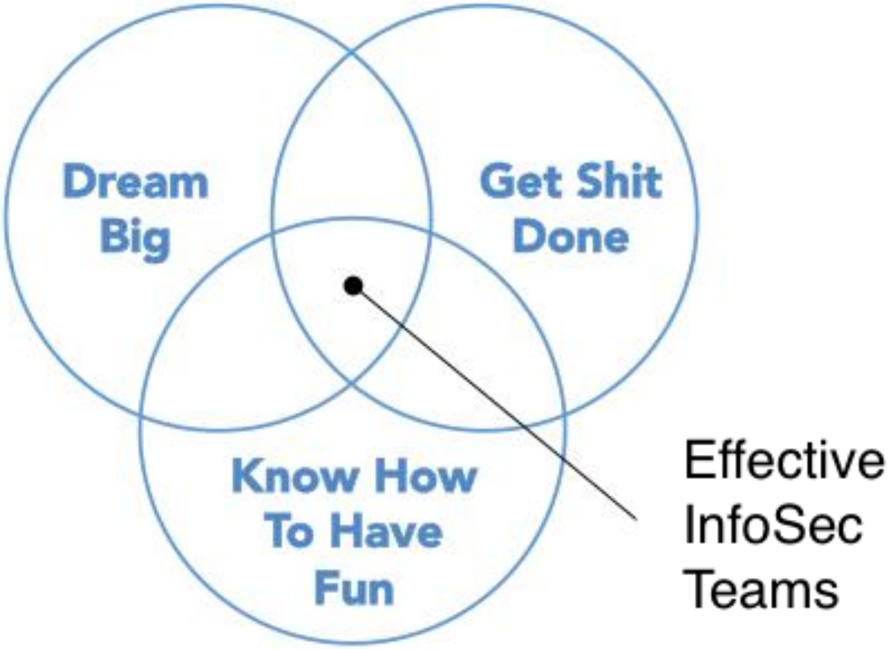
Likes: Flying planes

Dislikes: Automatic towel dispensers

Who do you want to work with?



What security team do you want to work with?



Agenda

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

1. Lightweight and iterative

Example: API Review

Version 1: Catalog the request, ask three questions, with canned advice
Version 2: Add conditionals to potentially introduce design review
Version 3: Automated scan to find vulnerabilities

Let people know that while the process will change, the entry point will not.

2. Can demonstrably reduce risk for each action taken

Example: Staff performance and sprint plan gut checks

1. Does this prevent something bad from happening in the future?
2. Did it let us know about something bad happening that we didn’t know about already?
3. Does it put us on a clear-line path to stopping an existing bad thing from happening anymore?

- Do this for your work plan every sprint. If you don’t like the answers, change the plan.
- Do this for your team every quarter. Document the results and the deliverables. Distill the majority of your performance discussions down to these questions.

3. Focus on operational excellence, less on authority

Example: Measure every meaningful aspect of your assessment and incident response programs. Share those results far and wide.

Assessment Measurements (Quarterly)

- Completed assessments, broken down by:
  - infrastructure
  - member-facing production apps
  - corporate systems
  - microsites
- Number of bugs filed
- How many assessments completed before go-live

Ecosystem Measurements (Quarterly)

- Production-impacting bugs filed by discovery source and current status (status weekly)
- Production-impacting bugs resolved
- Critical bugs impacting members, including response times
- External vulnerability report statistics

A Digression on Authority & Buy-In

- Tactical security teams should act as consultancies with a governance mission that they keep relatively well concealed.
- How much buy-in do you need?
- You’ll encounter three camps of people:
  - Supporters
  - Followers
  - Resistance

4. Makes others move instead of wait

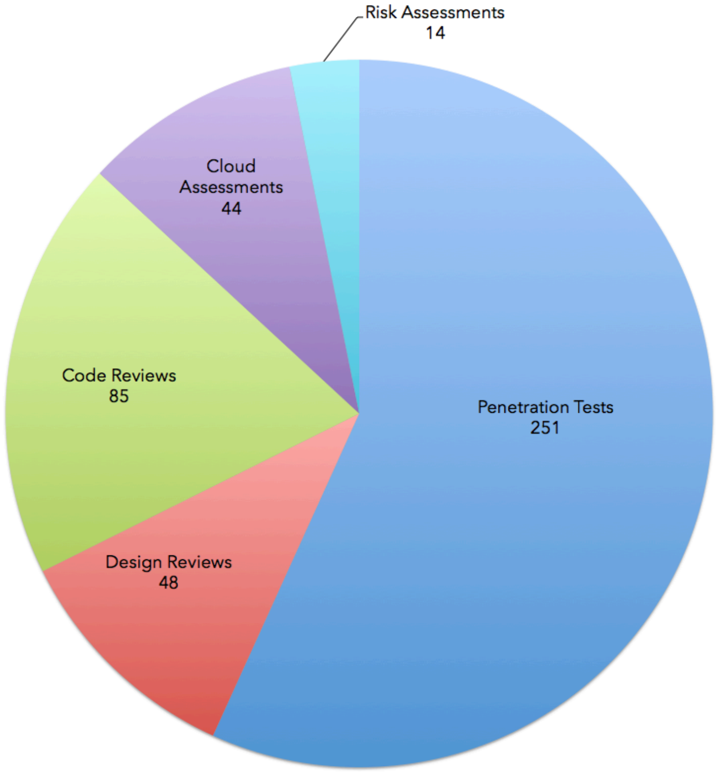
Example: First month on the job? I called a Code Yellow.

- Every team had a small amount of consistent work, tied to their sprints, monitored daily or weekly
- Prioritization discussions took place regularly, decisions on timing:
  - This sprint
  - This quarter
  - This year
  - Not sure

Agenda

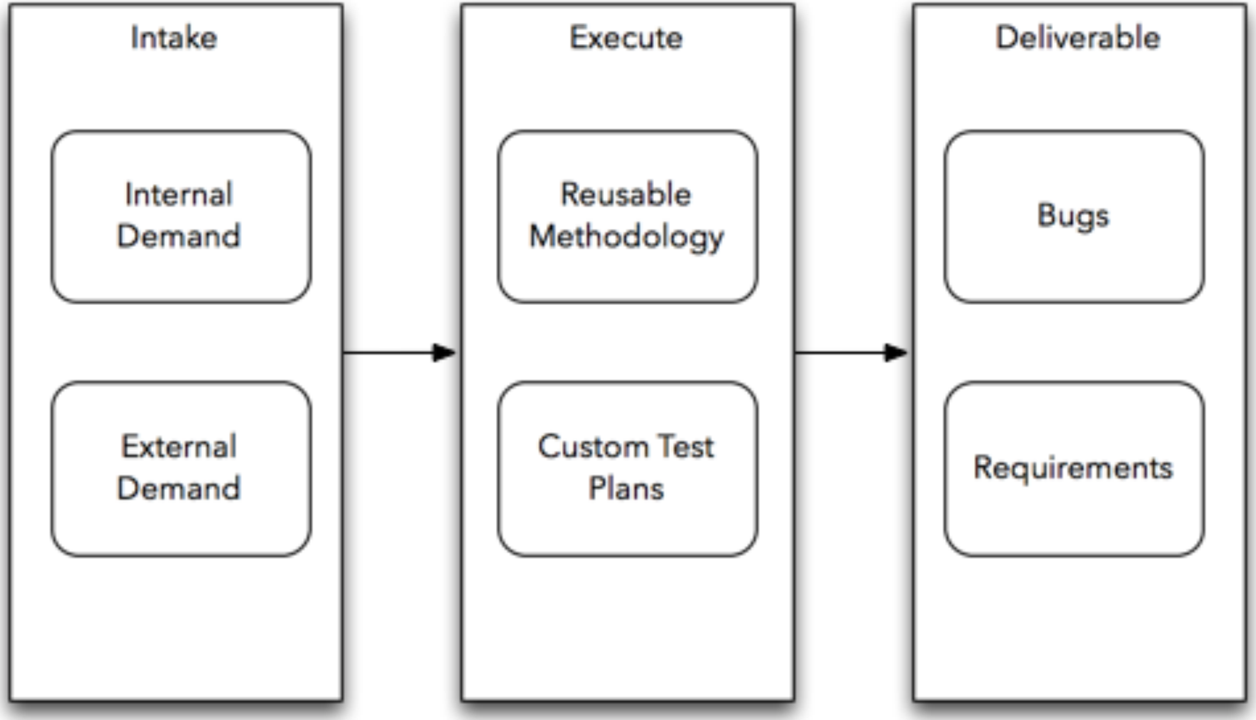
- Elements of a Tactical Security Program
- **Application Assessment**
- Application Incident Response
- Bug Bounty Programs

A Year Of Assessments At LinkedIn



Type	Number
Penetration Tests	251
Code Reviews	85
Design Reviews	48
Cloud Assessments	44
Risk Assessments	14

Assessments have a Flow



Intake

Internal Demand

External Demand

Execute

Reusable Methodology

Custom Test Plans

Deliverable

Bugs

Requirements

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.

An example office hours session

- Available twice a week, but can be scheduled on demand; signup sheet is the document of record
- House Security Team, Trust & Safety, and Product Legal, with a brief presentation by requestor
- We'll document requirements as we go
  - Product requirements: security, anti-abuse, legal
  - Assessment requirements: Next steps for deep dives, selections from the service catalog
- Each month, we do 30 product consultations, 25 general security sessions, and 4 corporate IT speed rounds

Assessment Tactics

- Build a service catalog. Here’s ours:
  - Threat model / risk assessment
  - Design review
  - Manual penetration test
  - Code review
  - Vendor review
- Document your methodology for consistency
- Scope each test and define game-overs
- Create test plans that include baseline methodology and specific test objectives

Navigating the wilderness of existential assessment questions

- What to do when you get what you think you wanted?
- Definitions can be hard. Don't avoid them. Own them instead.
  - What does review mean?
  - When are you done?
- How to deal with rapidly evolving products

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, communications & product marketing
    - Third-party assessments
    - 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

Agenda

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

Critical Security Bugs

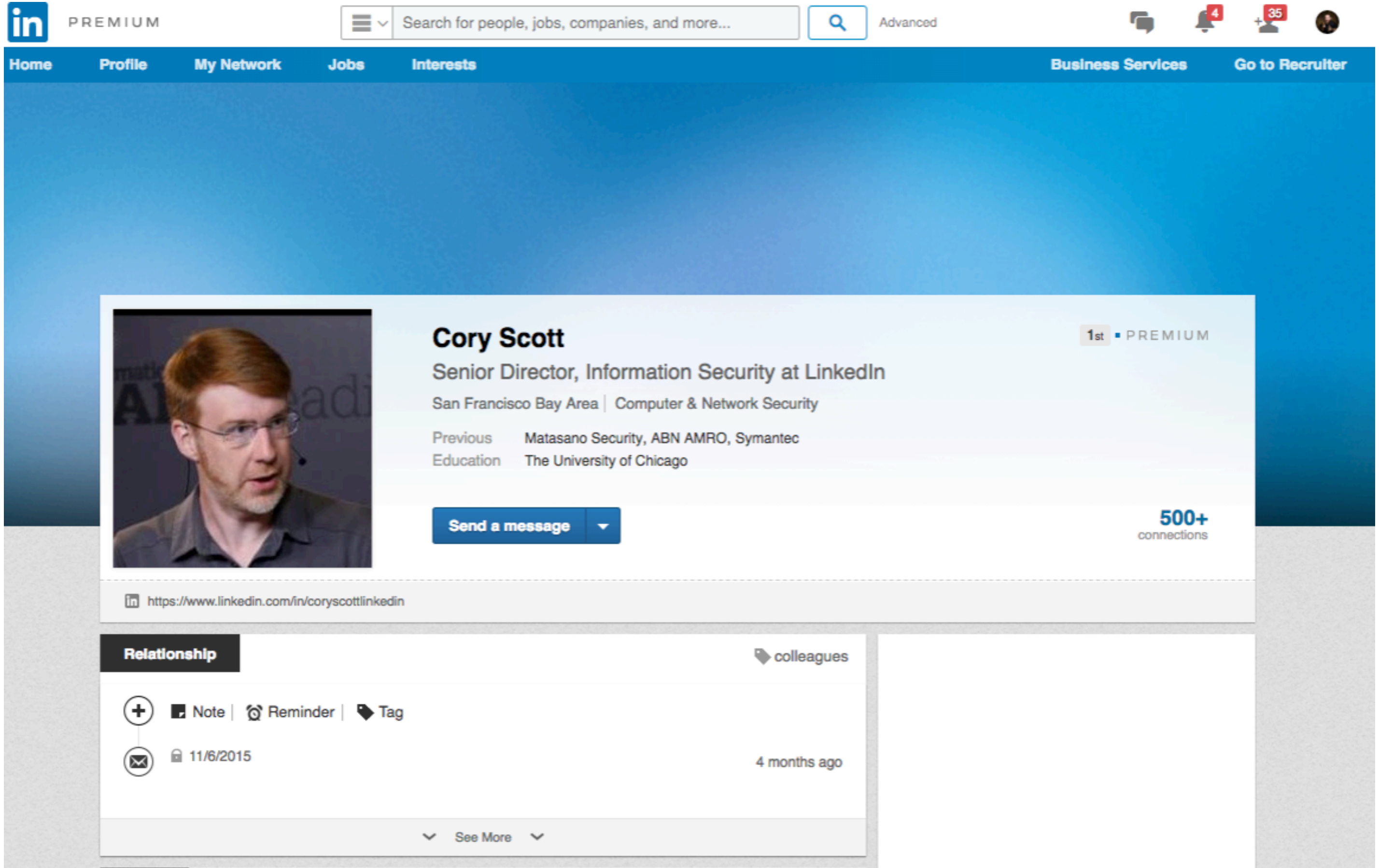
- 77 Critical bugs handled in the past year
  - 21 externally discovered
    - 13 from private bug bounty
    - 8 from other sources
  - 56 discovered internally
- We’ve been told that our definition of critical is more aggressive than the industry baseline.
- The vast majority of these bugs were closed without any member impact.

Handling Outside Reports

- 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
  - Establish working POC
  - File tickets
  - Respond
- 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...



Cory Scott

Senior Director, Information Security at LinkedIn

San Francisco Bay Area | Computer & Network Security

Previous Matasano Security, ABN AMRO, Symantec

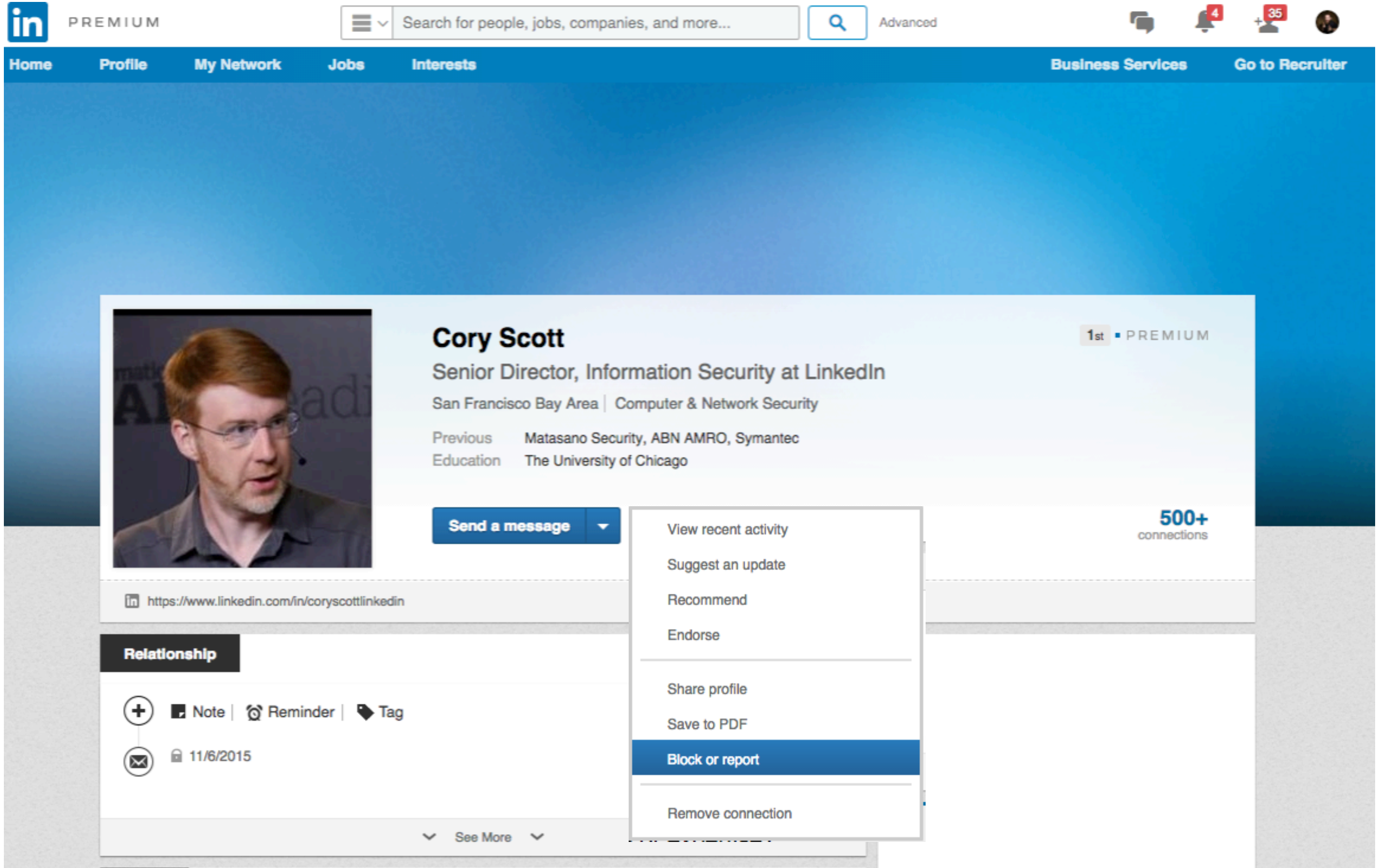
Education The University of Chicago

500+ connections

https://www.linkedin.com/in/coryscottlinkedin

colleagues

11/6/2015 4 months ago



Cory Scott

Senior Director, Information Security at LinkedIn

San Francisco Bay Area | Computer & Network Security

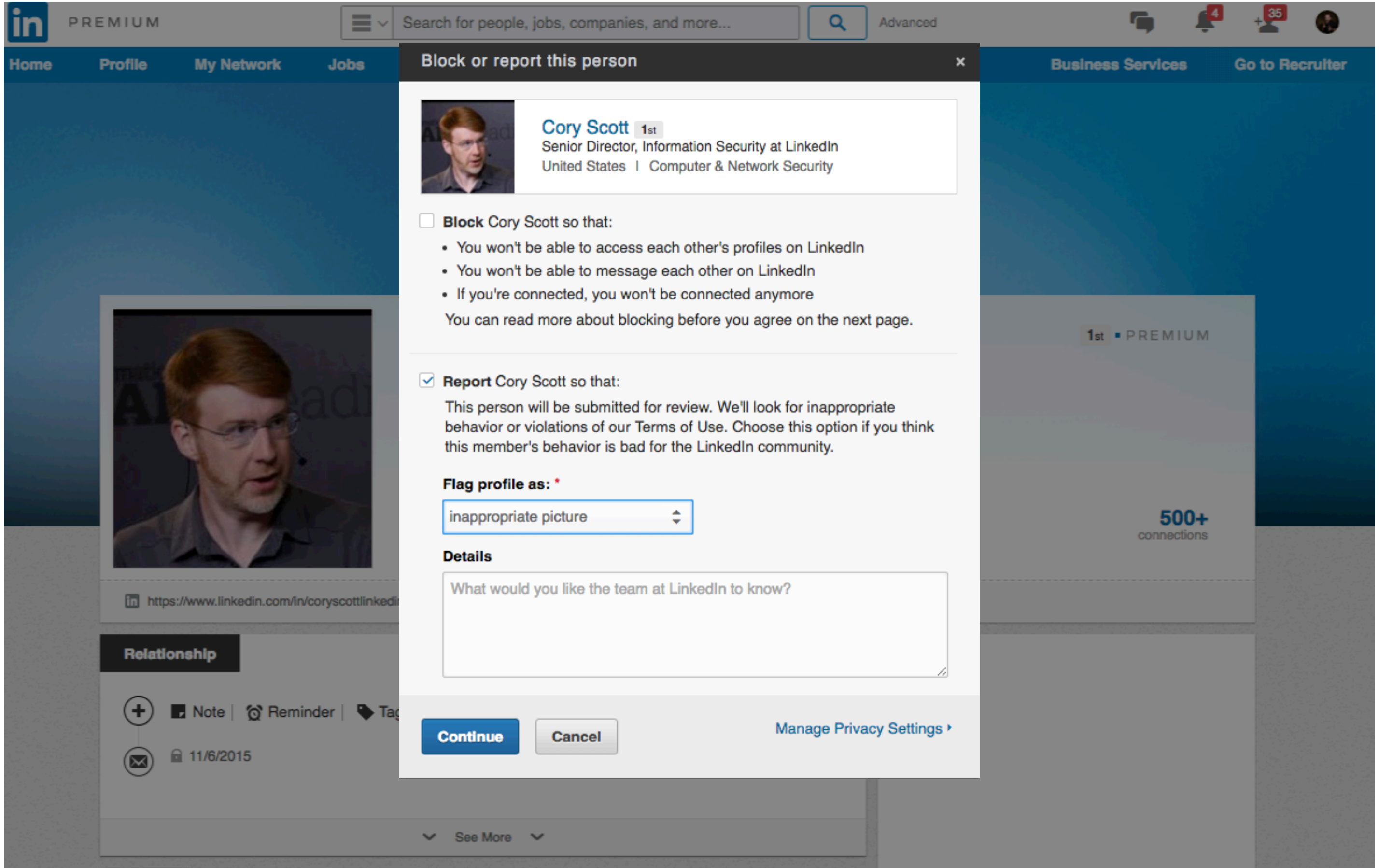
Previous Matasano Security, ABN AMRO, Symantec

Education The University of Chicago

500+ connections

https://www.linkedin.com/in/coryscottlinkedin

11/6/2015



Block or report this person

×

Cory Scott 1st
Senior Director, Information Security at LinkedIn
United States | Computer & Network Security

□ **Block** Cory Scott so that:

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore

You can read more about blocking before you agree on the next page.

☑ **Report** Cory Scott so that:

This person will be submitted for review. We'll look for inappropriate behavior or violations of our Terms of Use. Choose this option if you think this member's behavior is bad for the LinkedIn community.

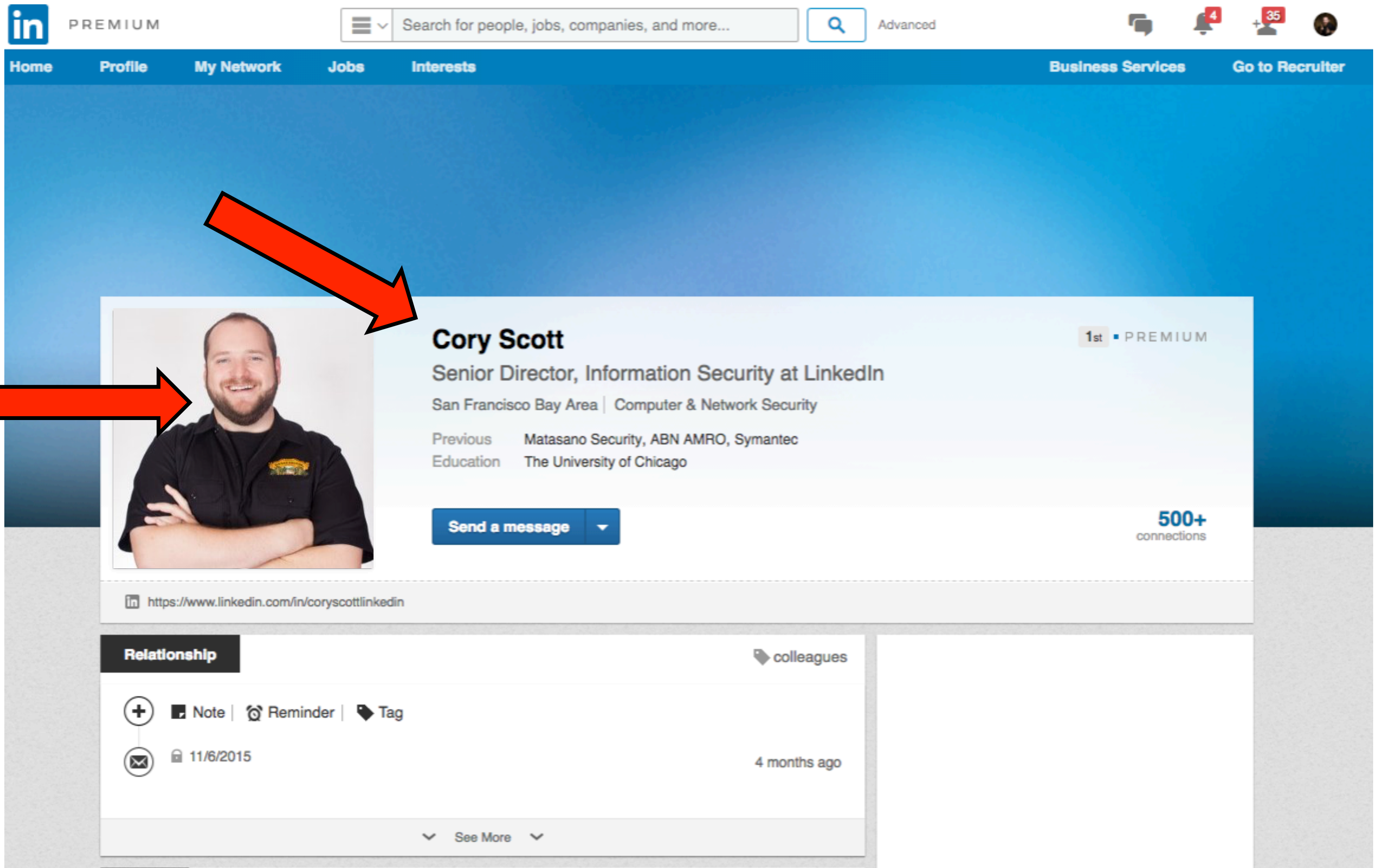
Flag profile as: *

inappropriate picture

Details

What would you like the team at LinkedIn to know?

Much Improved!



Cory Scott

1st · PREMIUM

Senior Director, Information Security at LinkedIn

San Francisco Bay Area | Computer & Network Security

Previous Matasano Security, ABN AMRO, Symantec

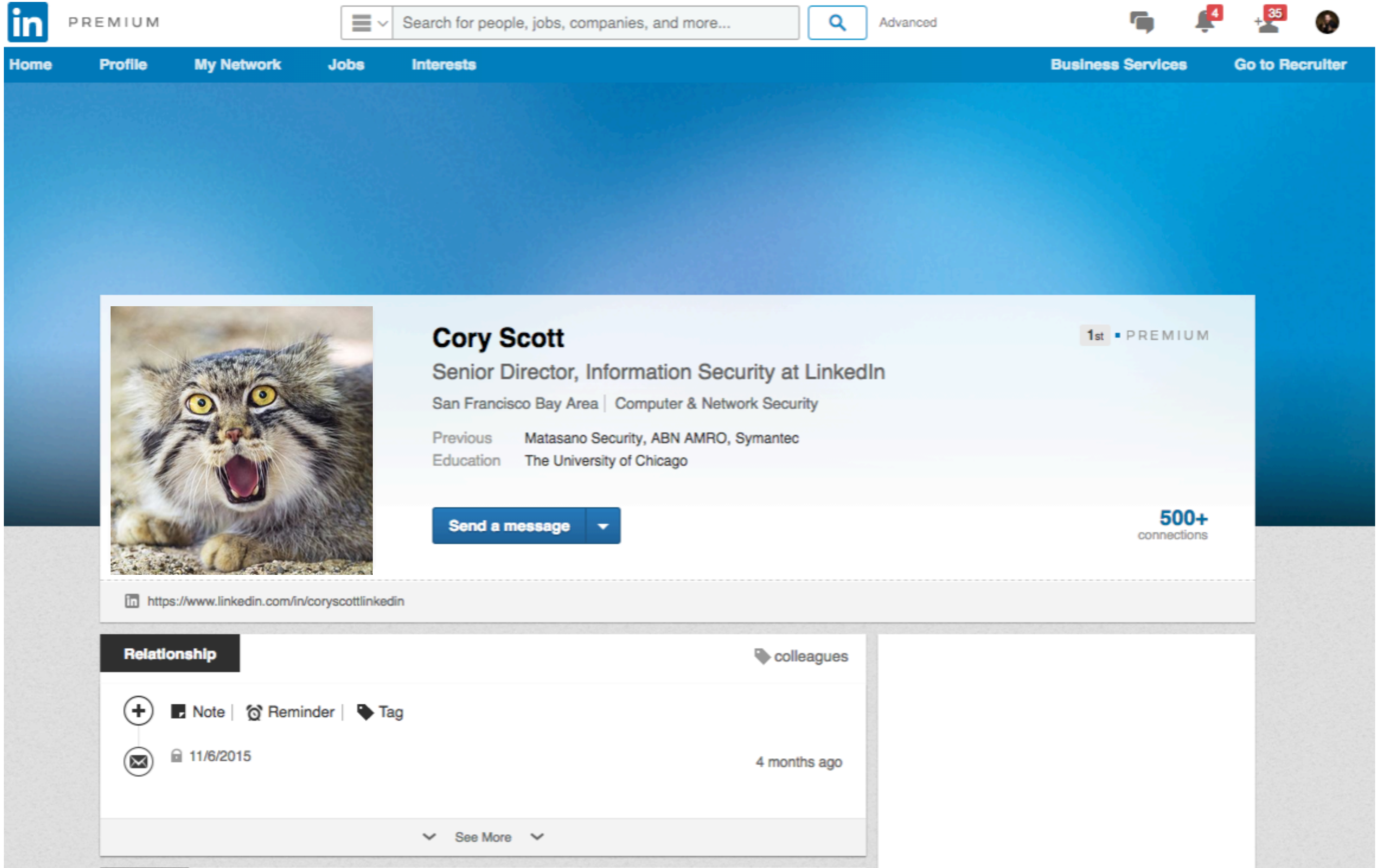
Education The University of Chicago

500+ connections

https://www.linkedin.com/in/coryscottlinkedin

colleagues

11/6/2015 4 months ago



Cory Scott

Senior Director, Information Security at LinkedIn

San Francisco Bay Area | Computer & Network Security

Previous	Matasano Security, ABN AMRO, Symantec
Education	The University of Chicago

500+ connections

https://www.linkedin.com/in/coryscottlinkedin

colleagues

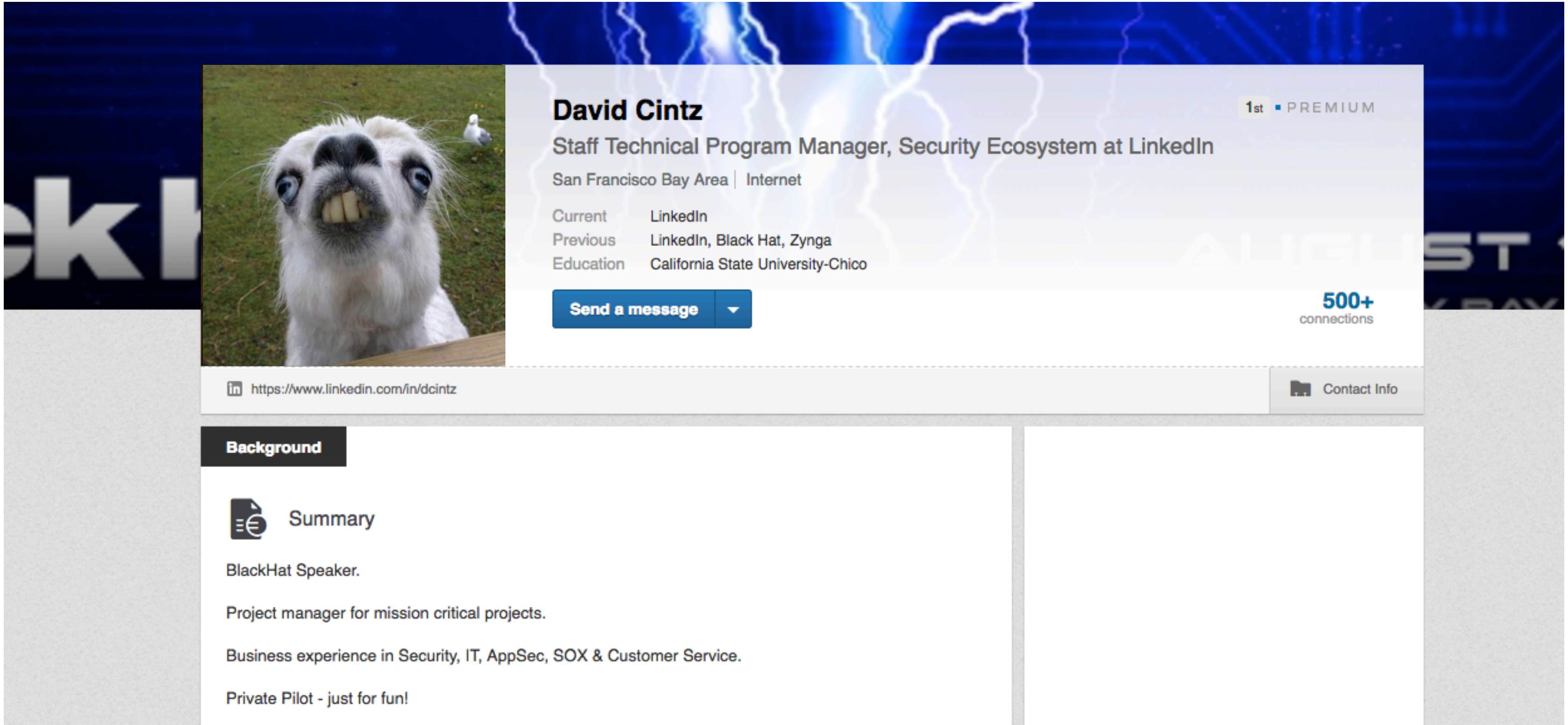
11/6/2015

4 months ago

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



David Cintz

Staff Technical Program Manager, Security Ecosystem at LinkedIn

San Francisco Bay Area | Internet

Current	LinkedIn
Previous	LinkedIn, Black Hat, Zynga
Education	California State University-Chico

500+ connections

https://www.linkedin.com/in/dcintz

Summary

BlackHat Speaker.

Project manager for mission critical projects.

Business experience in Security, IT, AppSec, SOX & Customer Service.

Private Pilot - just for fun!

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.

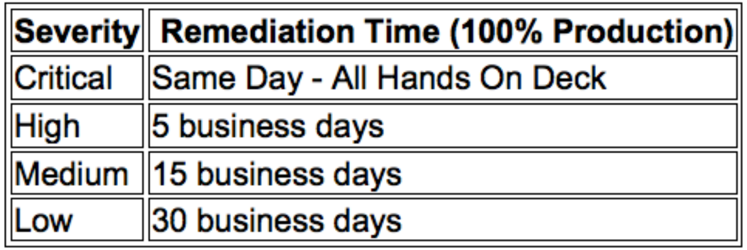
Case Study

- Externally reported through our bug bounty program
- Demonstrated that he could delete any embedded video from any SlideShare *(a LinkedIn company)* 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

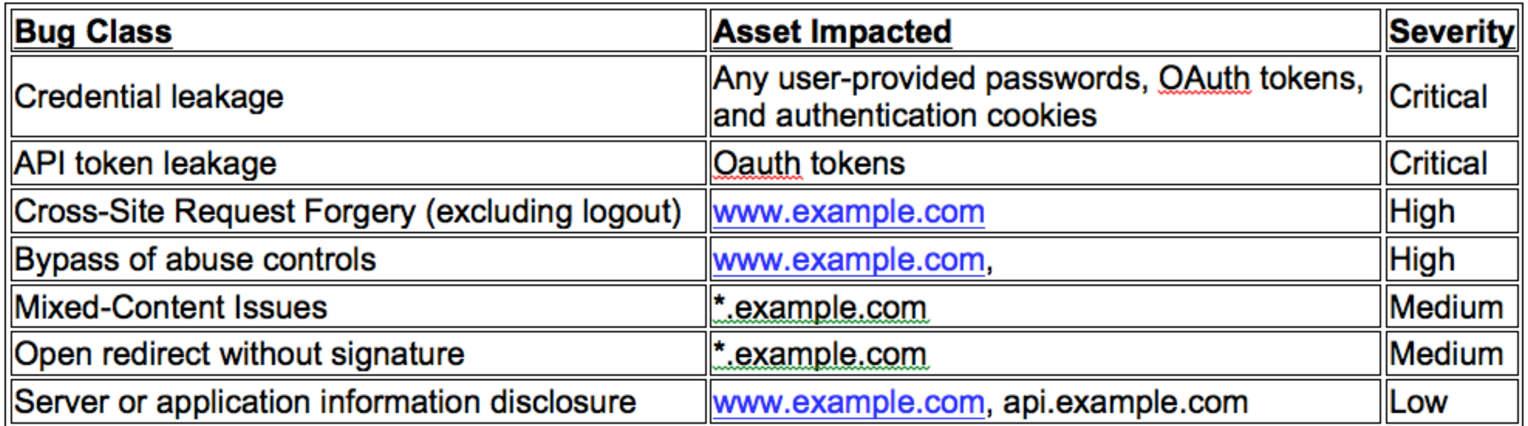
Bug Classifications and Why We Built It

- We/You are the face of security within your company
- We have to convince internal teams 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
  - Exploitability
  - “It has existed like that for years”

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
Cross-Site Request Forgery (excluding logout)	www.example.com	High
Bypass of abuse controls	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

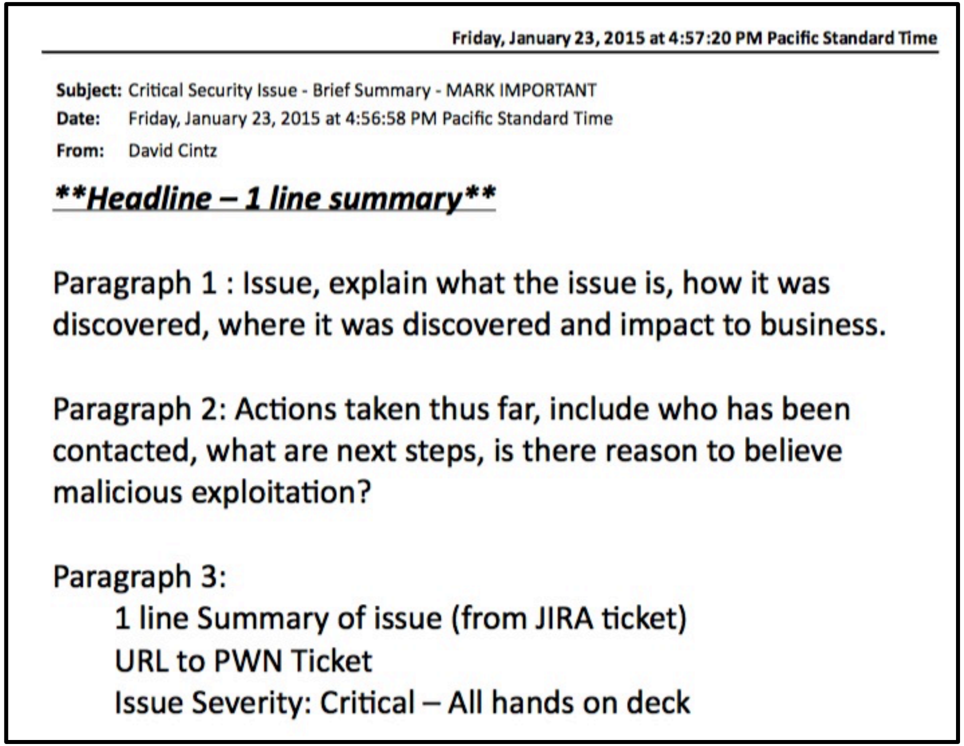
Importance of Communication During an Incident

- 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)

Communication Email Template



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

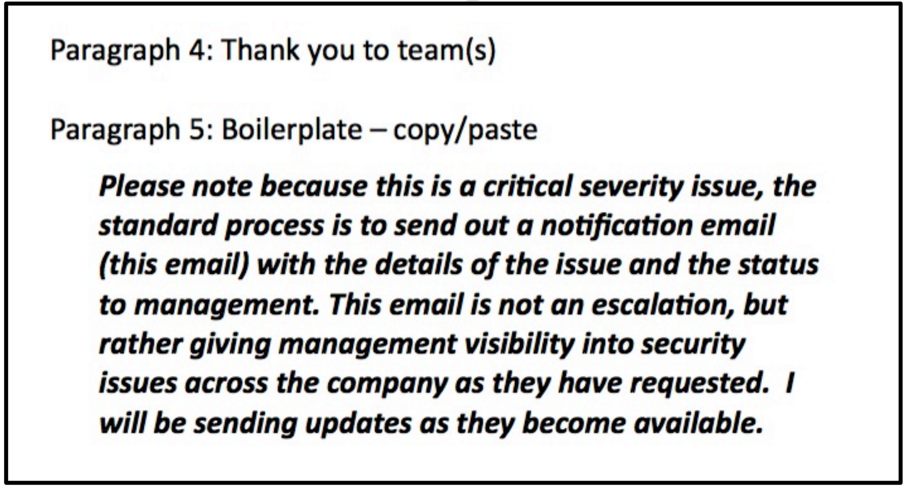
Subject: Critical Security Issue - Brief Summary - MARK IMPORTANT
Date: Friday, January 23, 2015 at 4:56:58 PM Pacific Standard Time
From: David Cintz

*****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.***

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

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**

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
- Signal to noise ratio constantly degrading
  - Companies forced to use dedicated resources
  - Engage consultancies
  - Use platform vendor to sift through the chaff

Case Study

- External researcher published a blog post about Intro product
- We opted to talk with the author
  - Did NOT involve legal
  - Reached out with a simple invite to chat
  - Goal was to work collaboratively
- These actions resulted in positive outcome
- 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.

How We Adopted Our Current Program

- Previously, a vast majority of reports to LinkedIn were not actionable or meaningful
- Smaller group of researchers emerged
- 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

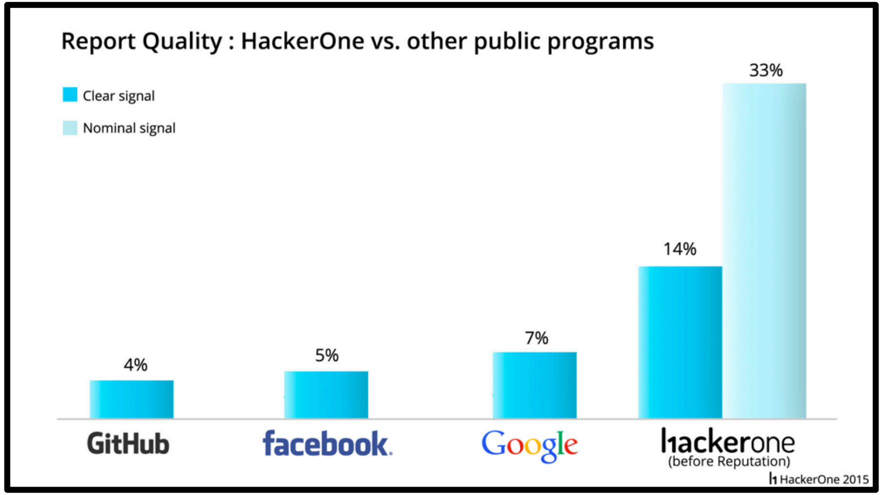
LinkedIn Program Now

- Launched LinkedIn private program 2015
  - Paid out over $45,000 bounties
  - Received more than 60 actionable reports
  - Signal to noise ratio 7:3
- We have seen significant reduction in authorization-related issues
- Less “gamesmanship” of program - Public programs incentivize Junk reports

What Do These Ratios Really Mean to Me?!

- Industry average is approximately 1:20
- What if every report took 1 hour on average to triage?
- Sifting through the bad reports is costly

What Do These Ratios Really Mean to Me?!



Report Quality : HackerOne vs. other public programs

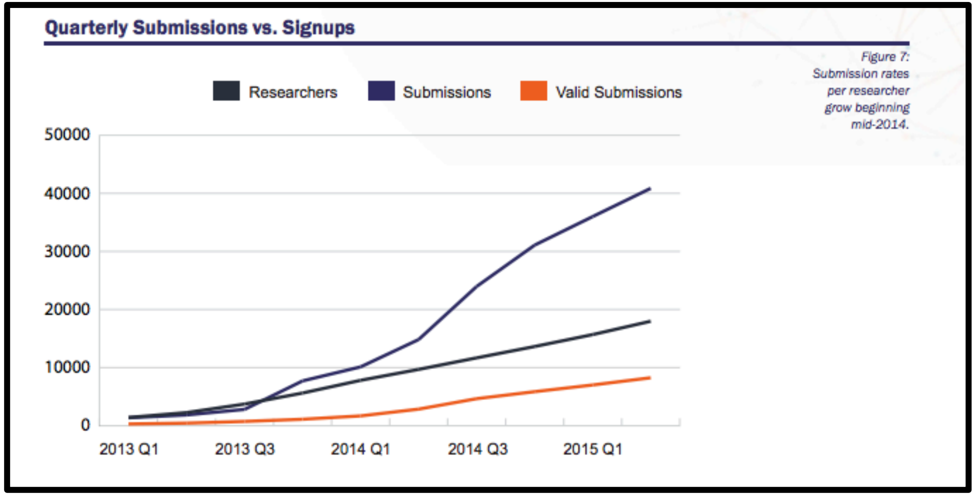
HackerOne 2015

HackerOne - July 2015

“Improving Signal Over 10,000 Bugs”

Bugcrowd - July 2015

“The State of Bug Bounty”



Quarterly Submissions vs. Signups

Figure 7: Submission rates per researcher grow beginning mid-2014.

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

Slides are at https://lnkd.in/getstuffdone

END