



Building a Product Security Team

The Good, the Bad and the Ugly – Lessons from the Field

Peter Morin



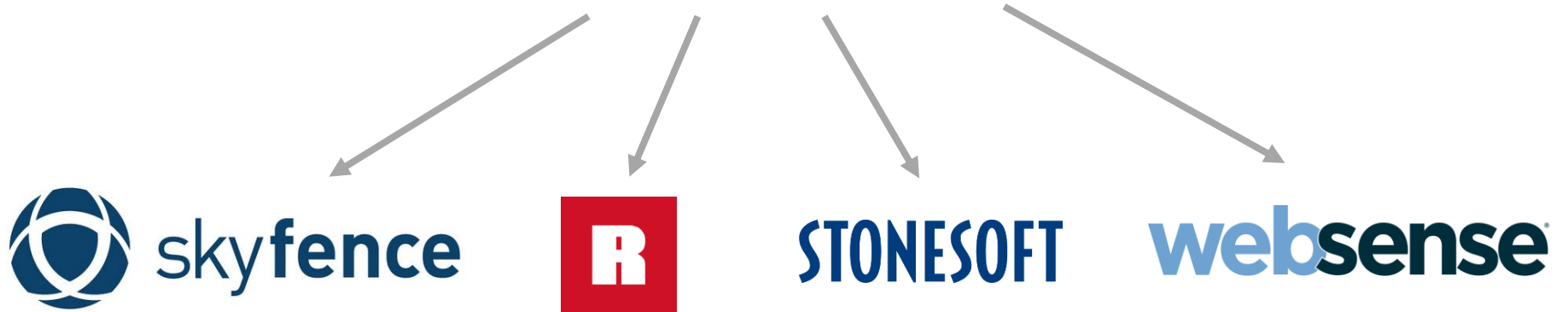
- Over 20yrs in the field
- Principal Cyber Engineer with Forcepoint
- Incident Response
- Worked in the past for the various military and government agencies
- Specialize in protection of critical infrastructure and DFIR

My Story

- I lead the Product Security Team for Forcepoint
- My career with Forcepoint started in December of 2015 at Raytheon
- Learned about what works and what doesn't
- Want to share my experiences
- Don't want to paint a bad picture – it is a **success story**



Raytheon



Forcepoint

- Many moving parts, numerous ways of doing things
- No one organization had a dedicated prod-sec effort
- Different people in the organization who thought they knew what product security should be
- 75+ products supported across the companies
- Raytheon having very structured security given its work with the US government and military

“We already do static code analysis with Coverity...”

”Not sure why we need a product security team, we hire third party testers every few years...”

”Engineering will decide when and how we fix security issues...”



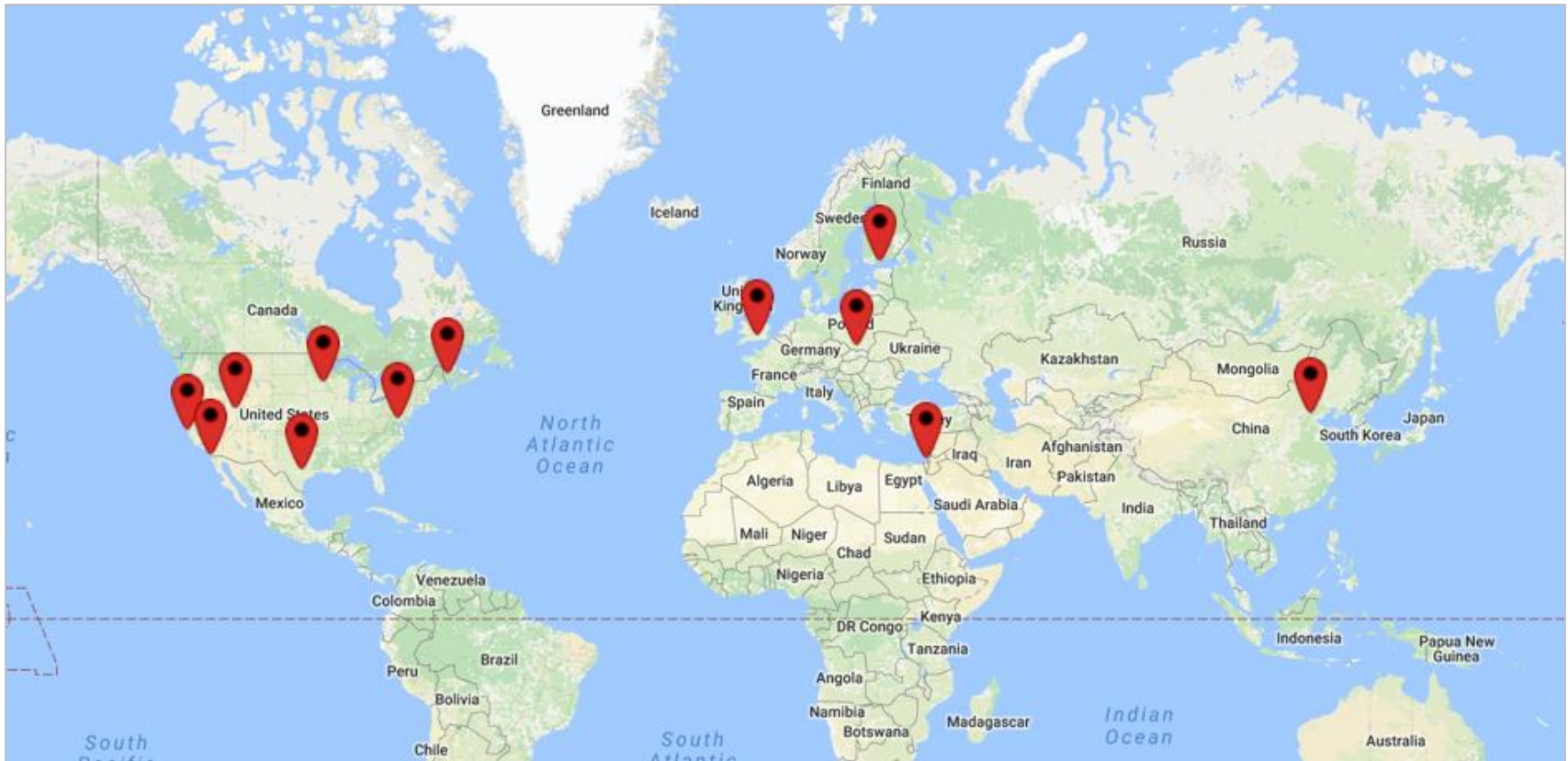
Selling Myself...

- **Hardest part of my whole story**
- At Raytheon, only a small number of people knew who I was and what my mandate was
- I was invisible to most
- People confused what I was doing with other Raytheon projects (i.e. Raytheon Code Center)
- Most were so tied up in strategizing, building, marketing and selling products

“At times it felt like I
could do **anything** but
also felt like I was
achieving **nothing...**”



Geographic Insanity



12 development centers over multiple time zones

Development Scariness

Development Environment



PERFORCE

Tech/Platforms



Do I Need Product Security?

- Does your company develop and sell software?
 - Packaged products, web applications, embedded software, mobile applications
 - Public consumption or custom built
- How are product security related vulnerabilities managed?
- Is your product tested for security flaws?



Product Security vs. Corporate Security

- **Corporate security**

- Tasked to defend and protect the enterprise
- Reports to a CISO, frequently IT department

- **Product security**

- Focuses on designing security into the products
- Frequently reports into engineering, CTO

Product Security vs. Corporate Security

- **Very different goals**
 - Can lead to conflicts or compromise of each others goals
 - Two security incidents reported nearly at the same time – one team has to decide, protect the corporation or protect the customer



Product Security vs. Corporate Security

- **Very different skills**
 - Producing a product involves all the phases of engineering, from requirements gathering, to design, development, and testing
 - Product security engineers involved in writing security requirements, code reviews, vulnerability testing
 - Corp. security involved in network design, deployment of off-the-shelf products, etc.

Product Security vs. Corporate Security

- **Different budgets**

- Sharing budgets can be very difficult due to different goals
- Separated teams allow the two budgets to be created and consumed without concern to the others
- Product security budgets can also factor into larger engineering/dev budgets

Creating a Program

- So you have decided to build a product security team
 - Defined mission
 - Defined program
 - Leadership support/sponsorship
 - Budget
 - Headcount



Building a Culture of Security

- Most important thing you need to start
- Not tools, people, budget, etc.
- **You need an executive sponsor that will champion your cause**
- Someone with an ear to the ground who has everyone's attention and is willing to put you in front of influential people



Building a Culture of Security

- Get everyone on board
- Present a story
- Show all the shortfalls that others have had
- Use real-world examples
- I met with VPs and directors (i.e. marketing, product management)

The screenshot shows a news article from 'SALTED HASH- TOP SECURITY NEWS' by Steve Ragan. The main headline is 'Researcher discloses zero-day vulnerability in FireEye'. Below the headline is a large image of a server rack with blue lights. To the right of the main image is a 'MORE LIKE THIS' section with three article thumbnails: 'Researcher to FireEye: If you're not paying, I'm not talking', 'Security companies shouldn't be this thin-skinned', and 'Hard-coded credentials placing dental offices at risk'. Below the main image is a sub-headline: 'NoSQL databases scale by adding more nodes. The costs of operations can add up very quickly.' and a paragraph: 'The researcher says that there are three other undisclosed flaws, and each one is for sale'. At the bottom right is a blue banner with the AT&T logo and the text 'Decoding the Adversary'. The article is dated 'CSO | Sep 6, 2015 11:41 PM PT'.

Mission Statement

FORCEPOINT™ PSIRT

The mission of the Forcepoint PSIRT is to establish, **oversee** and **carry out plans of action** for **any vulnerability** that potentially **threatens** the **confidentiality, integrity** or availability of **Forcepoint's products and services**.



Global team assisting customers with the ongoing security of their networks through **identification, resolution** and **prevention of vulnerabilities in Cisco products and industry-wide vulnerabilities**.

Defined Program

- What do I offer? What can I offer?
- You need bookends
- Need to set expectations early on
 - Response (i.e. vulnerability management, researchers)
 - Testing (i.e. penetration testing, code review, efficacy)
 - Design, architecture and consulting
 - Training
 - Research and development
 - Create and publish advisories and notices

Defined Program

- Know (and define) your constituency
 - Who are your customers?
 - Do researchers contact you? Media?
 - Don't forget internal customers (i.e. account reps, product management, engineering teams, QA teams, technical support, etc.)



Reporting Structure

- Where to be in the org chart to institute change?
- Will you report to CTO, CISO, CIO, director?
- Important that you report to someone who shares a similar mission
- Certain reporting structures could be red flags (i.e. IT)
- Can you be bypassed, by who?
- Veto power?



Headcount - Leadership

- Security bugs are not found unless actively sought out — it is hard work to institutionalize this type of scrutiny
- Ensure that engineers are not punished and keep them coming to security for advice
- When the team goes into incident response mode this role should be the calm champion

Headcount – Response Analyst

- Focused on responding to incidents
- Needs to have a very good understanding of the product (SME)
- Someone with good customer interaction skills
- Works well under pressure
- Strong interpersonal and leadership skills
- Strong analytical & evaluative thinking

Headcount - Breaker

- Focused on tearing apart your product
- Can show you if something is resilient to an attack or not.
- You'll ask "is this secure?" to this person frequently.
- The most entry level breaker may not even be able to write code at all and could still surprise a seasoned software engineer with an exploit.

Headcount - Fixer

- Lives for troubleshooting critical bugs, owning the commit, and identifying the short term fix
- They're all over the codebase and become that broad knowledge base of how the product works
- This role in a lot of cases may be a dotted line into an engineering team

Headcount – Program Manager

- Optional – may be needed as the team and responsibilities grow
- Managing testing schedules & the SDLC integration – staffing, etc.
- Scheduling external consultant reviews (i.e. contracts)
- Managing the overall success of various programs.



Building a Product Security Team: **Building Blocks of a PSIRT**

Know Your Product

- Know the product you are supporting inside out - shadow engineers, use the product, etc.
- If you don't understand the product, you can't be expected to find the flaws
- Slows down the response speed
- You will need access to the software – may require a lab to be established



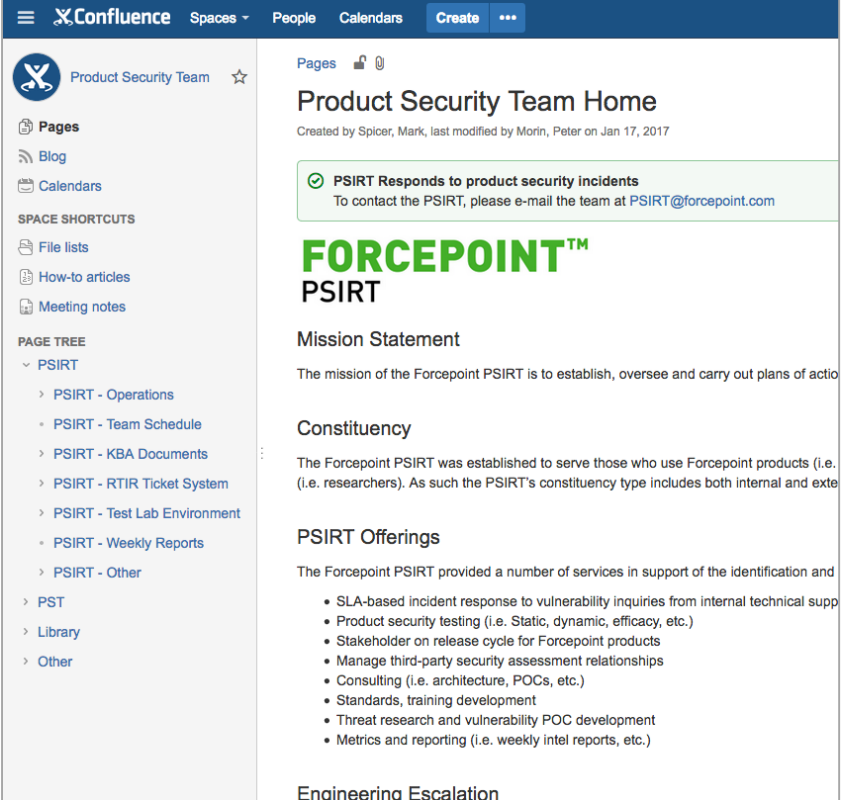
**KEEP
CALM
AND KNOW
YOUR
PRODUCT**

Policies & Processes

- Make sure these are “company” policies and not simply your policies
- Incident response SLAs
- Engineering patch development SLAs
- EOL policy
- Exception process
- Secure coding standards
- How to engage the product security team
- Disclosure policies

Policies & Processes

- Very critical that you document the process
- Make it available
- Invalidate all old processes
- Share this with everyone in the organization
- Ensure they sign-off that they understand it
- Have your executive sponsor enforce it



The screenshot shows a Confluence page titled "Product Security Team Home" for the "Product Security Team" space. The page includes a navigation sidebar with sections for Pages, Blog, Calendars, Space Shortcuts (File lists, How-to articles, Meeting notes), Page Tree (PSIRT, PST, Library, Other), and a main content area. The main content area features a green banner for "PSIRT Responds to product security incidents", the "FORCEPOINT™ PSIRT" logo, a "Mission Statement" section, a "Constituency" section, a "PSIRT Offerings" section with a bulleted list of services, and an "Engineering Escalation" section.

Product Security Team Home
Created by Spicer, Mark, last modified by Morin, Peter on Jan 17, 2017

✓ PSIRT Responds to product security incidents
To contact the PSIRT, please e-mail the team at PSIRT@forcepoint.com

FORCEPOINT™
PSIRT

Mission Statement
The mission of the Forcepoint PSIRT is to establish, oversee and carry out plans of action

Constituency
The Forcepoint PSIRT was established to serve those who use Forcepoint products (i.e. researchers). As such the PSIRT's constituency type includes both internal and external

PSIRT Offerings
The Forcepoint PSIRT provided a number of services in support of the identification and response to security incidents

- SLA-based incident response to vulnerability inquiries from internal technical support
- Product security testing (i.e. Static, dynamic, efficacy, etc.)
- Stakeholder on release cycle for Forcepoint products
- Manage third-party security assessment relationships
- Consulting (i.e. architecture, POCs, etc.)
- Standards, training development
- Threat research and vulnerability POC development
- Metrics and reporting (i.e. weekly intel reports, etc.)

Engineering Escalation

Testing Your Product

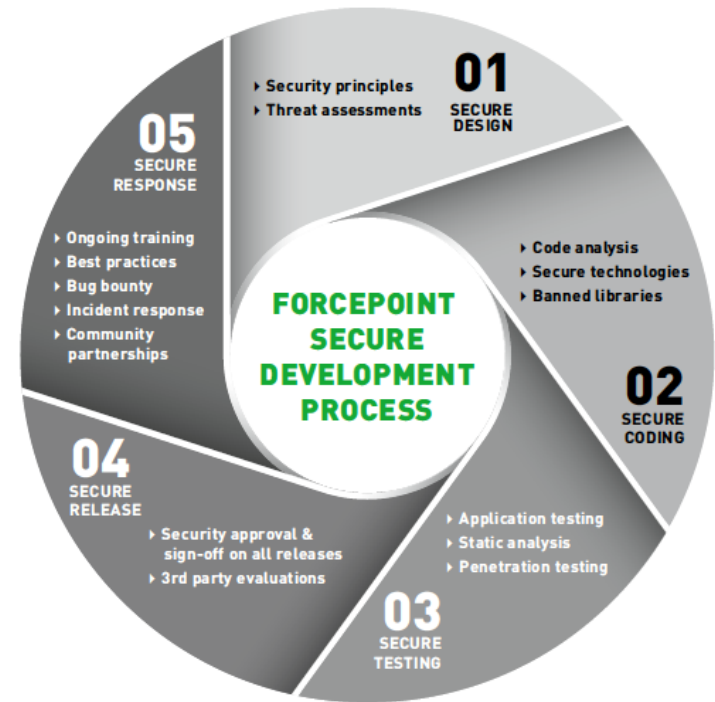
- You will have to determine a number of key items to be successful in testing:
 - Test plan – are you following a process?
 - Scope – what are you testing?
 - Resourcing – do you have the right people?
 - Scheduling (i.e. when, how often) – SDLC integration should determine this
 - Reporting – who is the audience?

Testing Your Product

- Many methods (static code, dynamic/pen, efficacy, etc.)
 - Are you planning on integrating your testing with the build cycle / continuous integration
- Use a standard (OWASP, NIST, OSSTM, etc.)
- Many tools out there (i.e. AppScan, Webinspect, Burp, Fortify, Checkmarx, etc.)
 - Be aware, these are expensive – you will need budget

Security and the SDLC

- Initially you will find testing your product prior to release is all you will be able to handle
- Eventually you want to be integrated into the SDLC
- Will involve being involved in design, requirements, etc.
- **You need to own this - not engineering**
- In many cases your customers will want to see a process like this in place



Security and the SDLC - Transparency



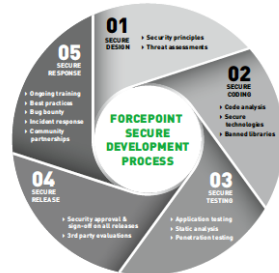
Developing Vulnerability Resistant Products



FORCEPOINT™
Trust Program



At Forcepoint™, we know that secure products and services are essential for organizations to perform and succeed in an ever more challenging threat environment. The Forcepoint Trust Program was created to establish the highest level of trust and confidence with our customers and the security community. Led by our Product Security Team, the Forcepoint Trust Program ensures that security is part of every phase of our software development lifecycle and that transparency is maintained in how we handle security.



Developing Vulnerability Resistant Products

Our commitment to the security of our products and services can be found throughout our product lifecycle and includes key elements such as:

- Product Security involvement in the design and architecture of Forcepoint products
- Investment in experienced security personnel, cutting edge technology, and ensuring our products are secure
- Rapid response to security issues
- Ensuring transparency in our security processes and research

To ensure that security, our trust, and our products are developed with the highest level of security, we perform penetration testing, our products are developed with security in mind, we provide engineers with the tools and resources they need to succeed, we engage with external security experts, and most importantly, we are most involved in our security.

- Security is developed with the highest level of security
- We perform penetration testing
- Our products are developed with security in mind
- We provide engineers with the tools and resources they need to succeed
- We engage with external security experts
- Most importantly, we are most involved in our security



Exploitation

The objective of this step is to exploit the vulnerabilities identified in previous steps. This is done by using several databases documenting known exploits, including any internally-identified zero-day exploits, trying to obtain unauthorized access to the systems. Our testers analyze the previously-identified vulnerabilities and develop an attack strategy. It is, of course, intrusive by the nature of the activities carried out. During this phase, testers are focused on identifying common security flaws that lead to exploitation such as:

- Remote code execution
- Privileged escalation
- Buffer overflow

We subject our security solutions to real-world attacks, which is critical to reducing the threat surfaces of our products.

DYNAMIC APPLICATION SECURITY TESTING (DAST)

Dynamic application security testing involves testing the application from the outside in - by examining the application in its running state and attempting to manipulate it in unexpected ways in order to discover security vulnerabilities. This type of testing identifies highly-exploitable vulnerabilities such as SQL injection and cross-site scripting. It also finds runtime issues that can't easily be found by looking at code in its offline state via static analysis, such as authentication issues, server misconfiguration issues and vulnerabilities that are only visible when you log in as a known user.

Figure 2 - Forcepoint Dynamic Application Security Testing Approach



Whitepaper

Forcepoint™ Secure Testing Methodology

Forcepoint™ Secure Testing Methodology

Information Gathering

During this step, the tester is focused on gaining a clear understanding of how the application functions - its interaction with the user and other systems. Various "discovery" exercises are performed, including web spidering, user-directed spidering, brute force scanning, etc.

Configuration Management

This step focuses on assessing the infrastructure used in the delivery of the application (e.g. Tomcat, Apache) as well as any database systems used to store application data (e.g. MongoDB, MySQL) for potential security vulnerabilities that may lead to reducing the overall integrity of the application.

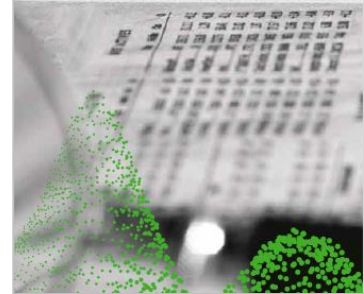
Application Testing (e.g. Authentication, Session Management)

The goal of these steps is to identify any application-based vulnerabilities that could potentially be exploited. These vulnerabilities are identified using both automated scanning and enumeration tools, such as IBM AppScan, Burp Suite Professional and OWASP ZAP, as well as manual review procedures. The application testing step focuses on the review of the following areas:

- Client-side controls
- Authentication and authorization mechanisms (e.g. roles and permissions)
- Session management mechanisms
- Input-based filtering
- Business logic
- Use of third-party libraries (e.g. node.js, Angular.js)
- Application interfaces (e.g. REST)

During this phase, testers are focused on also identifying common web application security flaws including:

- SQL injection
- Path traversal
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (CSRF)



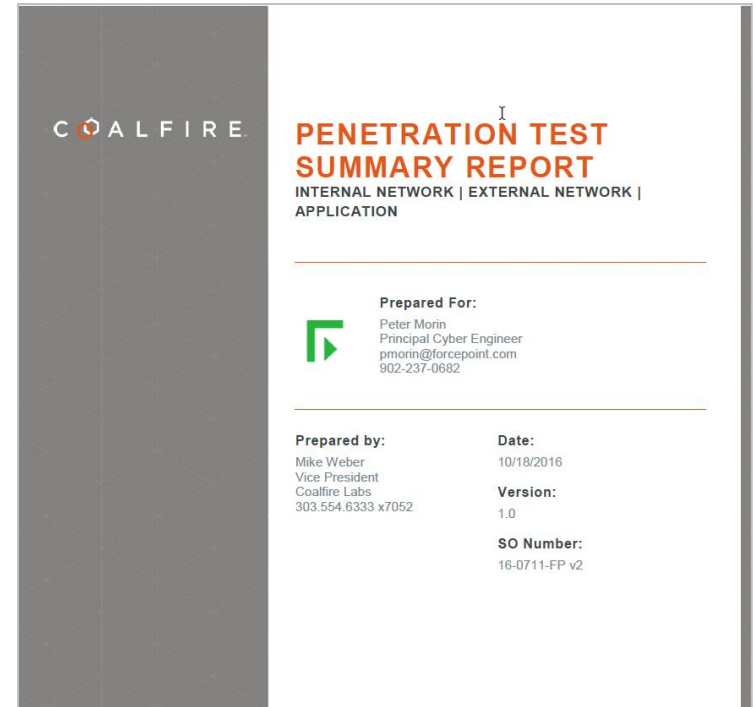
Alliances & Champions

- Work to gain confidence from other groups within your organization
- Offer lunch and learns, etc.
- Organize events such as internal bug bounties
- Make yourself available
- Highlight employees who are helping to win for you
- You cannot be successful without the rest of the organization contributing



When to use a third party tester?

- Can be useful, though expensive, and could be never ending
- We do these for each major release
- Good way to have third party validation
- Engagement should be management by prod-sec
- Have third party prepare an “external” version of the report
- Alternate between third parties year to year.



Measuring Your Success

- We produce a weekly report for executive management
 - Threat research & intel
 - New incidents
 - New KBAs released
 - New hotfixes and updates
 - Open tickets with status
 - App vs. third party



Perception is Key

- How are you marketed outside the organization?
- How are you perceived by researchers
- How do you deal with disclosure?
- External advertising of your PSIRT (website, e-mail, etc.)

Backlash after Oracle IT security executive Mary Ann Davidson pens 'nuttty' 3000-word rant mocking customers for trying to find its security flaws

Liam Tung Show comments

[f SHARE](#) [TWEET](#) [✉](#) [MORE](#)

Oracle, the company behind one of the most vulnerable products on the web, has told customers to fix their own security problems before trying to find flaws in Oracle products.

Oracle's chief information security officer Mary Ann Davidson ruffled a few feathers on Tuesday in a 3000-word rant detailing how it scolds customers who reverse-engineer its products to find bugs that may undermine the security of their own systems.



[SHARE](#)

CURE CUSTOMER BORN
with the entertainment the
Offers
\$10
DIRECTV FOR BUSINESS
START

MOST POPULAR

- 1 Credit card fraud: 8 ways you can be hijacked
- 2 Speed check: what your NBN promises mean
- 3 This algorithm lets you bet or without ever watching
- 4 NSW Police using spyware on WikiLeaks data
- 5 Australians making the most

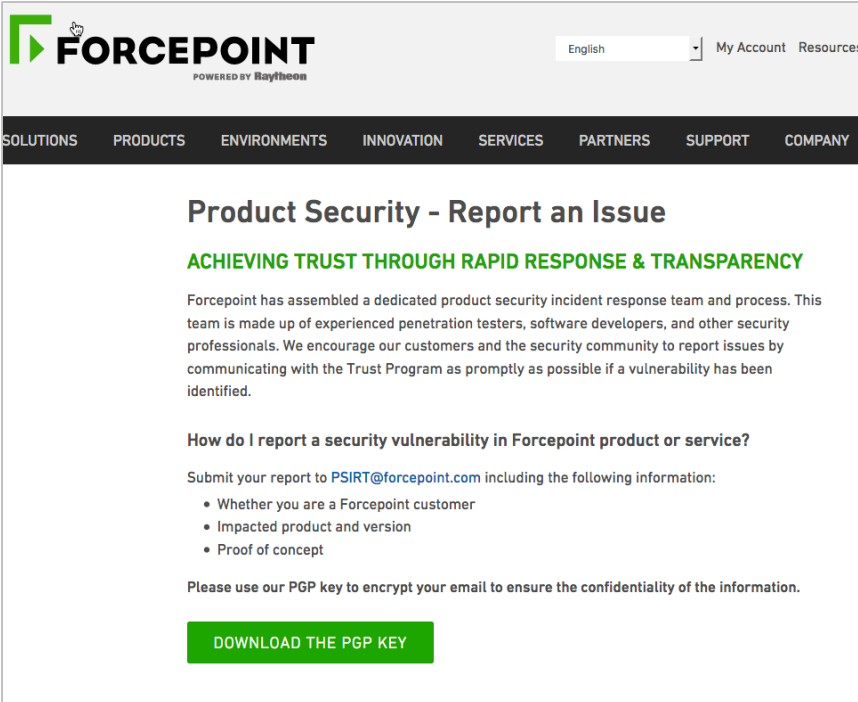
Perception is Key

- What about researchers?
 - Embargos (fixing before disclosing)
 - Make sure you know what engineers and product management can offer prior to negotiating with researchers
 - You need to know what you can bargain with



Perception is Key

- Communications
 - **No response is a response**
 - Align with PR and legal – you will need them
 - Ensure they are not putting out statements without you – may contradict your program
 - Does prod-sec have a public presence?



The screenshot shows the Forcepoint website's product security page. At the top, the Forcepoint logo is displayed with the tagline 'POWERED BY Raytheon'. A navigation menu includes links for SOLUTIONS, PRODUCTS, ENVIRONMENTS, INNOVATION, SERVICES, PARTNERS, SUPPORT, and COMPANY. The main heading is 'Product Security - Report an Issue', followed by the sub-heading 'ACHIEVING TRUST THROUGH RAPID RESPONSE & TRANSPARENCY'. The text describes a dedicated incident response team and encourages reporting vulnerabilities. A section titled 'How do I report a security vulnerability in Forcepoint product or service?' lists required information: whether the reporter is a customer, the product version, and a proof of concept. A green button labeled 'DOWNLOAD THE PGP KEY' is provided for confidentiality.

Perception is Key

- Knowledge Base Articles
 - We use KBAs to communicate the status of vulnerabilities
 - Provide detailed info about security issues that involve our products and require an upgrade, fix, or other customer action
 - Critical that the public understand that you know the vulnerability exists and that you are assessing

The screenshot shows a Forcepoint Knowledge Base article. The header includes the Forcepoint logo (POWERED BY Raytheon) and navigation links for SUPPORT HOME, DOCUMENTATION, DOWNLOADS, and KNOWLEDGE BASE. The article title is 'CVE-2017-3136, CVE-2017-3137, CVE-2017-3138 BIND Security Vulnerabilities'. Below the title, it lists the article number (000012679), products (Sidewinder, Sidewinder Appliances, Sidewinder Virtual Appliance), version (8.3, 7.0), and last published date (Wed Apr 19 22:49:30 GMT 2017). The main section is 'PROBLEM DESCRIPTION', which includes a 'KBA Summary' and a 'Products Under Review' section. The 'Affected Products' section lists Forcepoint Sidewinder.

FORCEPOINT
POWERED BY Raytheon

My Account

SUPPORT HOME DOCUMENTATION DOWNLOADS KNOWLEDGE BASE

Home / Knowledgebase

CVE-2017-3136, CVE-2017-3137, CVE-2017-3138 BIND Security Vulnerabilities

Article Number: 000012679
Products: Sidewinder, Sidewinder Appliances, Sidewinder Virtual Appliance
Version: 8.3, 7.0
Last Published Date: Wed Apr 19 22:49:30 GMT 2017

PROBLEM DESCRIPTION

Published Date: April 17, 2017
Last Update: April 19, 2017
KBA Status: In Development
KBA Severity: Multiple levels; see below
CVE Numbers:
CVE-2017-3136 - Medium
CVE-2017-3137 - High
CVE-2017-3138 - Medium

KBA Summary

The Forcepoint Product Security Incident Response Team is investigating the following security vulnerabilities and their potential impact on Forcepoint products. This article will be updated after assessments and fixes are completed, if applicable.

Vulnerabilities in BIND include an error handling synthesized records; a response packet causing a resolver to terminate; and an exit with an assertion failure resulting from a null command string.

Products Under Review

- Forcepoint i500 Appliance (formerly i-Series appliance)
- Forcepoint Web Security Cloud and Forcepoint Email Security Cloud (formerly TRITON AP-WEB Cloud and TRITON AP-EMAIL Cloud)

Affected Products

- Forcepoint Sidewinder

Tracking...

- Important to track incidents as well as vulnerabilities
- Don't get hung up with other group's ticketing system
- You may need to deploy your own system given most don't adapt as well to IR work
- Also, we wanted a system we owned
- We ended up using RTIR



Tracking...



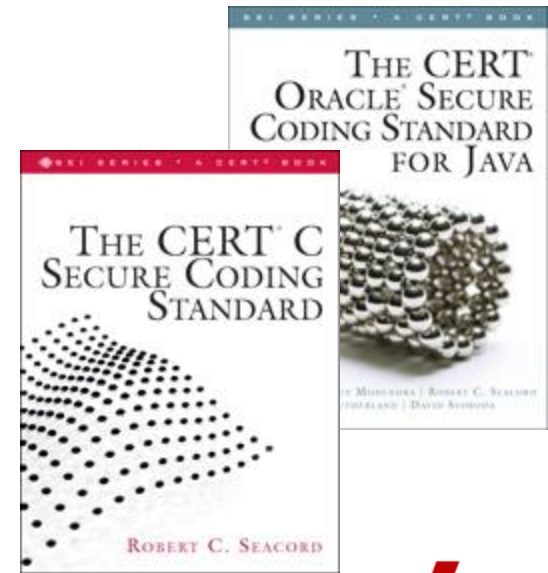
- We open RTIR ticket:
 - Initial incident report
 - All reporter info gets logged here
 - Track progress of incident



- We open a JIRA ticket if:
 - We need to escalate to engineering
 - We require a fix to be developed
 - Interact with engineering

Use Industry Standards

- Using industry standards will allow you to set a common structure throughout the organization
- Scoring vulnerabilities
- CVE, CWE, CVSS – will make it easy for others to understand this common “language”
- Other standards such as CERT Coding standards, SafeCode



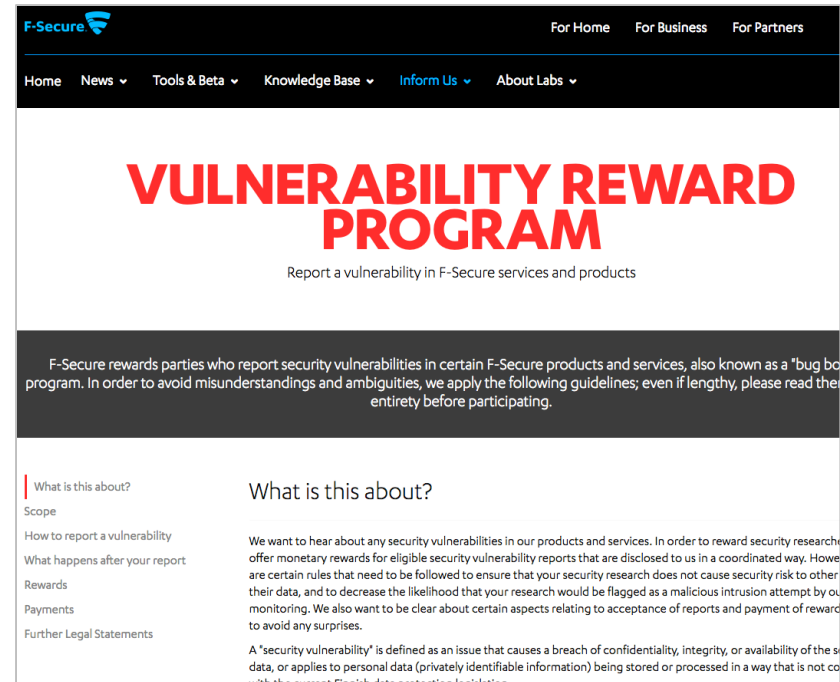
Community Involvement

- More you are involved with the community, the more the public will be aware of your company's prod-sec efforts
- Ensure your team is able to frequent events
- Promote public speaking in your team



Bug Bounty

- Start small – internal bug bounty
- Work with a trusted third party
- Some do it themselves...
- What you are prepared to offer?
- Remember bounties also bring a spotlight onto your organization
- Some people make a living off this
- Noticed researchers who come to us ask whether we have rewards



The screenshot shows the F-Secure Vulnerability Reward Program page. The header includes the F-Secure logo and navigation links for Home, News, Tools & Beta, Knowledge Base, Inform Us, and About Labs. The main heading is "VULNERABILITY REWARD PROGRAM" in large red letters, with the subtitle "Report a vulnerability in F-Secure services and products". Below this, a dark banner contains the text: "F-Secure rewards parties who report security vulnerabilities in certain F-Secure products and services, also known as a 'bug bounty' program. In order to avoid misunderstandings and ambiguities, we apply the following guidelines; even if lengthy, please read them in their entirety before participating." The main content area is split into two columns. The left column has a table of contents with links: "What is this about?", "Scope", "How to report a vulnerability", "What happens after your report", "Rewards", "Payments", and "Further Legal Statements". The right column has the heading "What is this about?" followed by a paragraph: "We want to hear about any security vulnerabilities in our products and services. In order to reward security researchers, we offer monetary rewards for eligible security vulnerability reports that are disclosed to us in a coordinated way. However, there are certain rules that need to be followed to ensure that your security research does not cause security risk to other users, their data, and to decrease the likelihood that your research would be flagged as a malicious intrusion attempt by our security monitoring. We also want to be clear about certain aspects relating to acceptance of reports and payment of rewards to avoid any surprises." Below this is a definition: "A 'security vulnerability' is defined as an issue that causes a breach of confidentiality, integrity, or availability of the system, or applies to personal data (privately identifiable information) being stored or processed in a way that is not compliant with the current Spanish data protection legislation."

In Closing

- **Best practices for success – in my humble opinion**
 - Operate with as much transparency as possible – will go along way with researchers and customers
 - Know your product inside and out
 - Find a good executive sponsor
 - Be persistent with your organization
 - show them the value of what you're trying to do!
 - Be an active part of the community



Questions? Comments?

Peter Morin

petermorin123@gmail.com

Twitter: @petermorin123

<http://www.petermorin.com>