30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

Crawl, Walk, Run: **Living the PSIRT Framework**

Mark Stanislav
Director of Application Security, Duo Security

FIRST™
Improving Security Together

Product Security Incident Response Team (PSIRT)

- Counterpart to a Computer Security Incident Response Team (CSIRT), not a replacement -- high-maturity organizations have both!

- A PSIRT is likely to establish functions that service both their internal stakeholders (e.g. engineers) and external parties (e.g. researchers).

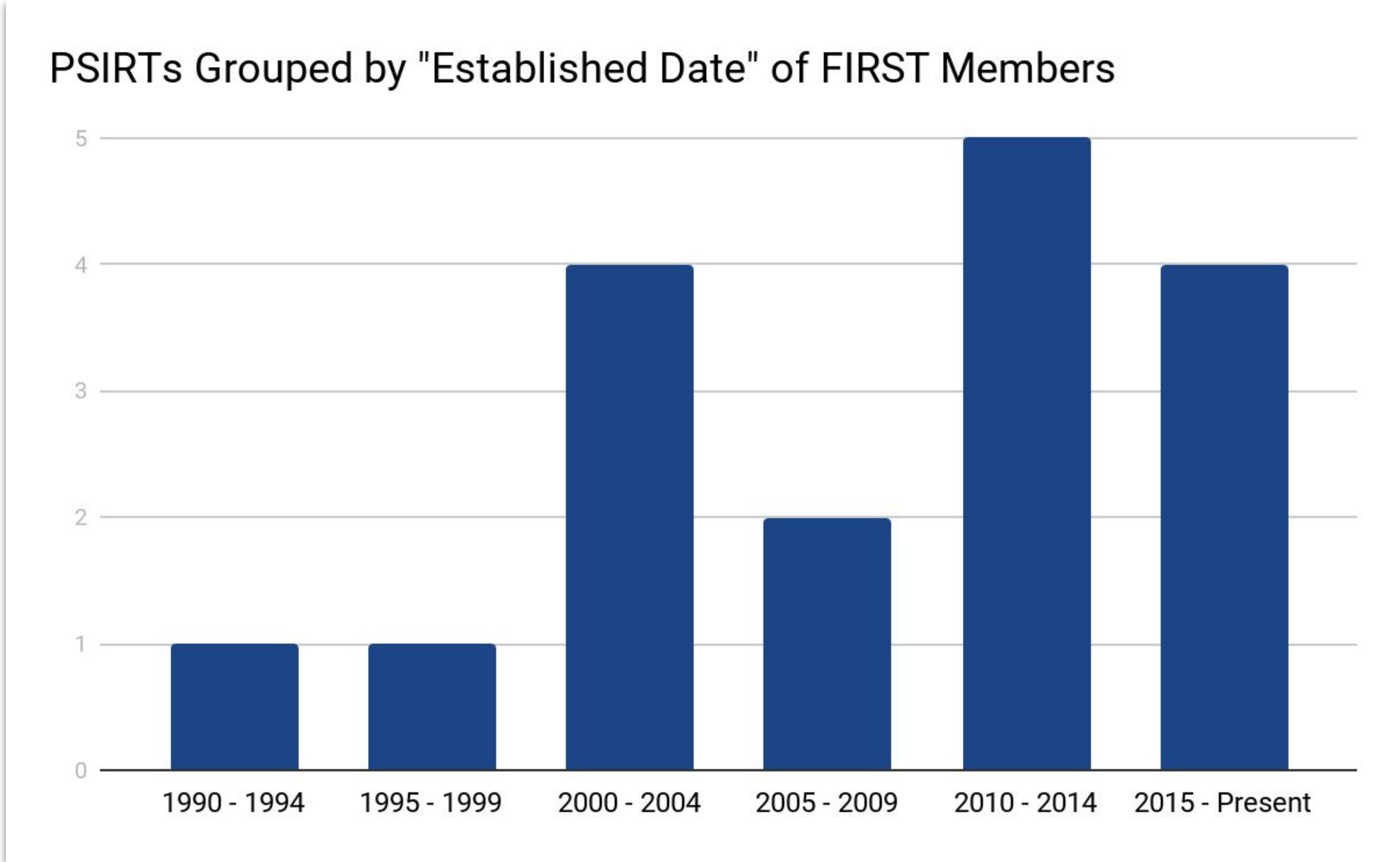
- Establishes a *programmatic* approach to managing the full scope of ensuring that products & services provided by their organization are able to resolve security defects and communicate risk to customers.

Understanding PSIRT Populations & Age

- FIRST has 17 members of 420 total with “product” in their team’s naming.

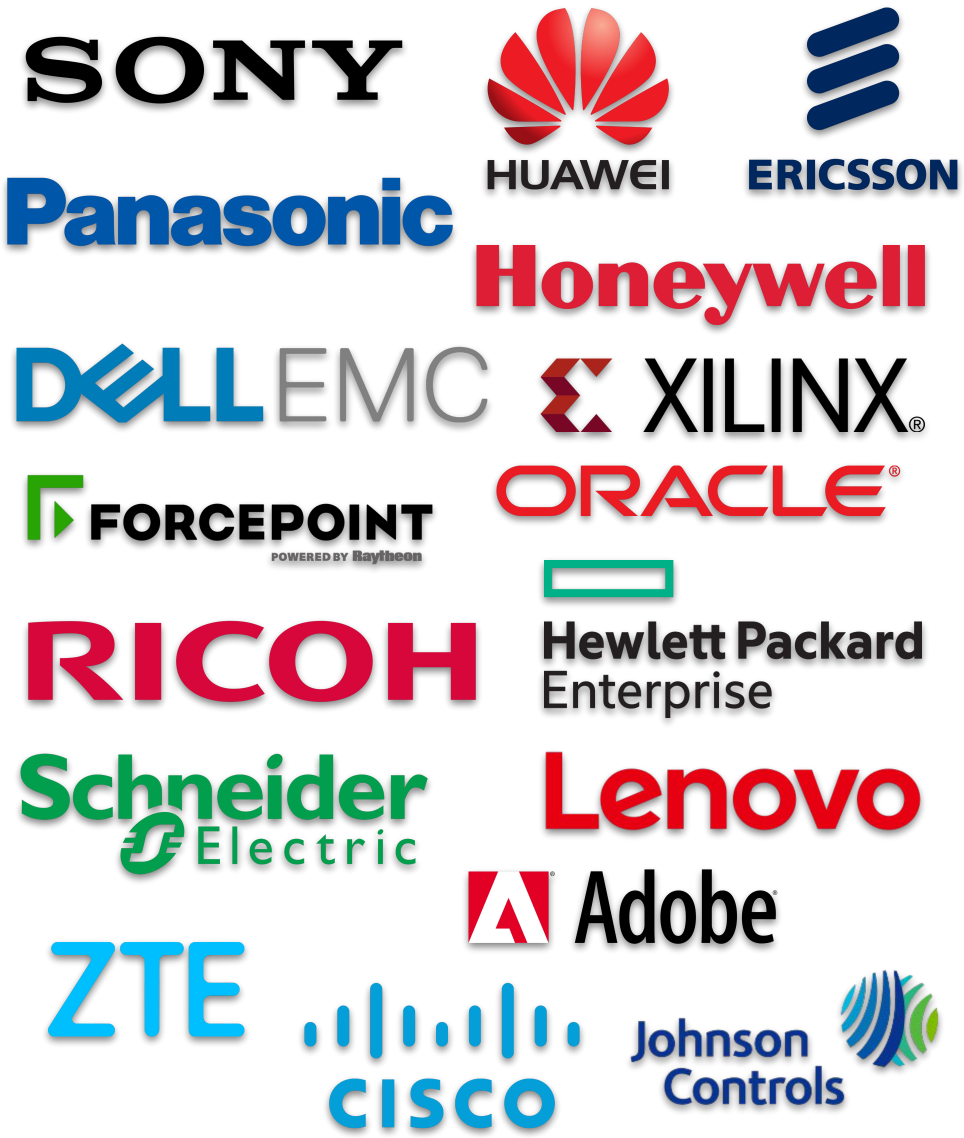
- The earliest established PSIRT is HPE in 1992!

- We’re clearly still in a nascent period of PSIRT.



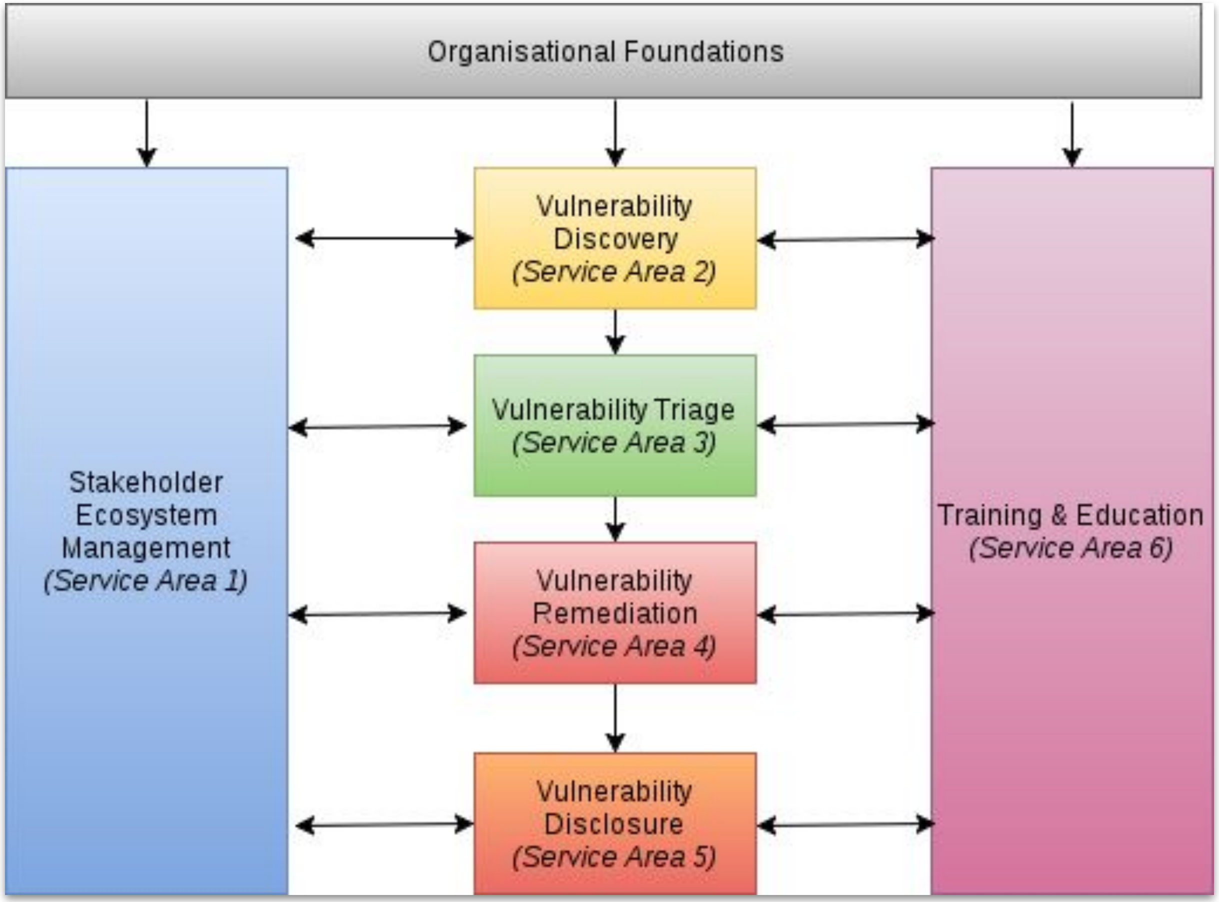
Why So Few PSIRTs?

- Data is *only* for ‘full’ members of FIRST, not an index of all that exist.
- Some organizations may choose not to break-out PSIRT cleanly.
- Others may just use their CSIRT as a conduit for FIRST involvement.
- All BIG names on this list...



The FIRST PSIRT Services Framework (v1.0 Draft)

- Released in draft form in June, 2017 to gain industry feedback.
  - Compliments the CSIRT Services Framework from March, 2016.
- Six defined "Service Areas" to group PSIRT focuses & process.
- The basis of this presentation!



Organisational Foundations

Stakeholder Ecosystem Management *(Service Area 1)*

Vulnerability Discovery *(Service Area 2)*

Vulnerability Triage *(Service Area 3)*

Vulnerability Remediation *(Service Area 4)*

Vulnerability Disclosure *(Service Area 5)*

Training & Education *(Service Area 6)*

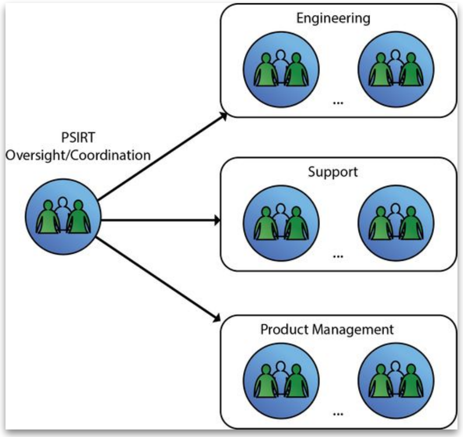
Services Framework Organizational PSIRT Models

- Intends to provide models that will satisfy many organizational sizes, maturity, and structures.

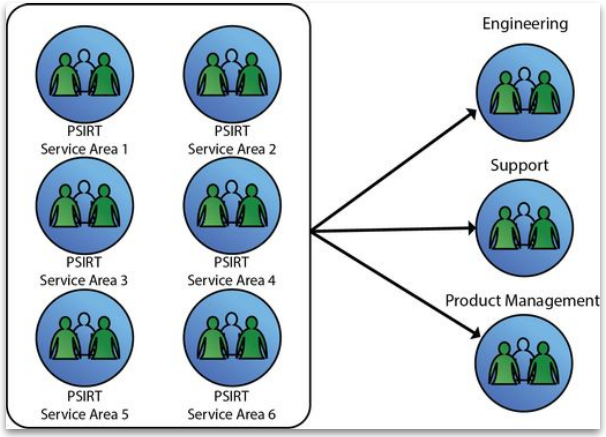
- Helps to frame the ownership of various key PSIRT functions.

- Focus on *success*, not trying to do square pegs->round holes.

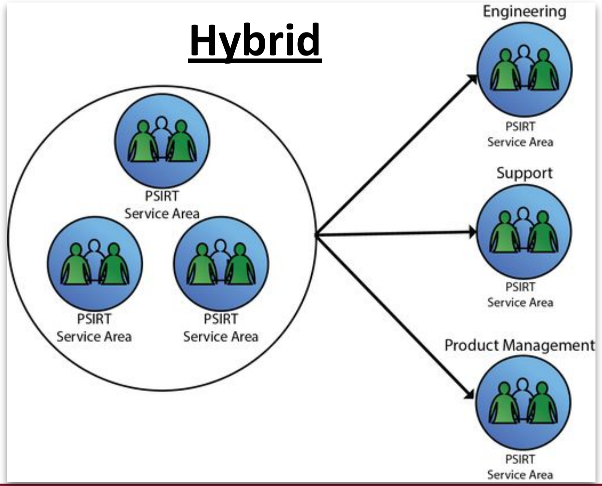
Distributed



Centralized



Hybrid

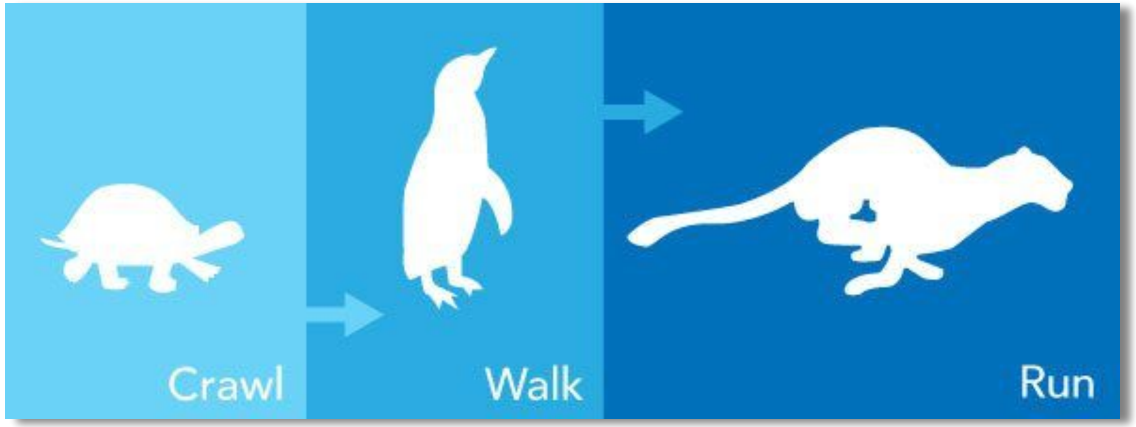


Product Security for the Rest of Us

- While dedicated PSIRT functions exist in large corporations, all of us responsible for product security should be building a program, too!

- 25% of LinkedIn job titles with “PSIRT” belong to just five companies.

Let’s Talk About How to Get to a Better Place!



Understanding DUO Product Security

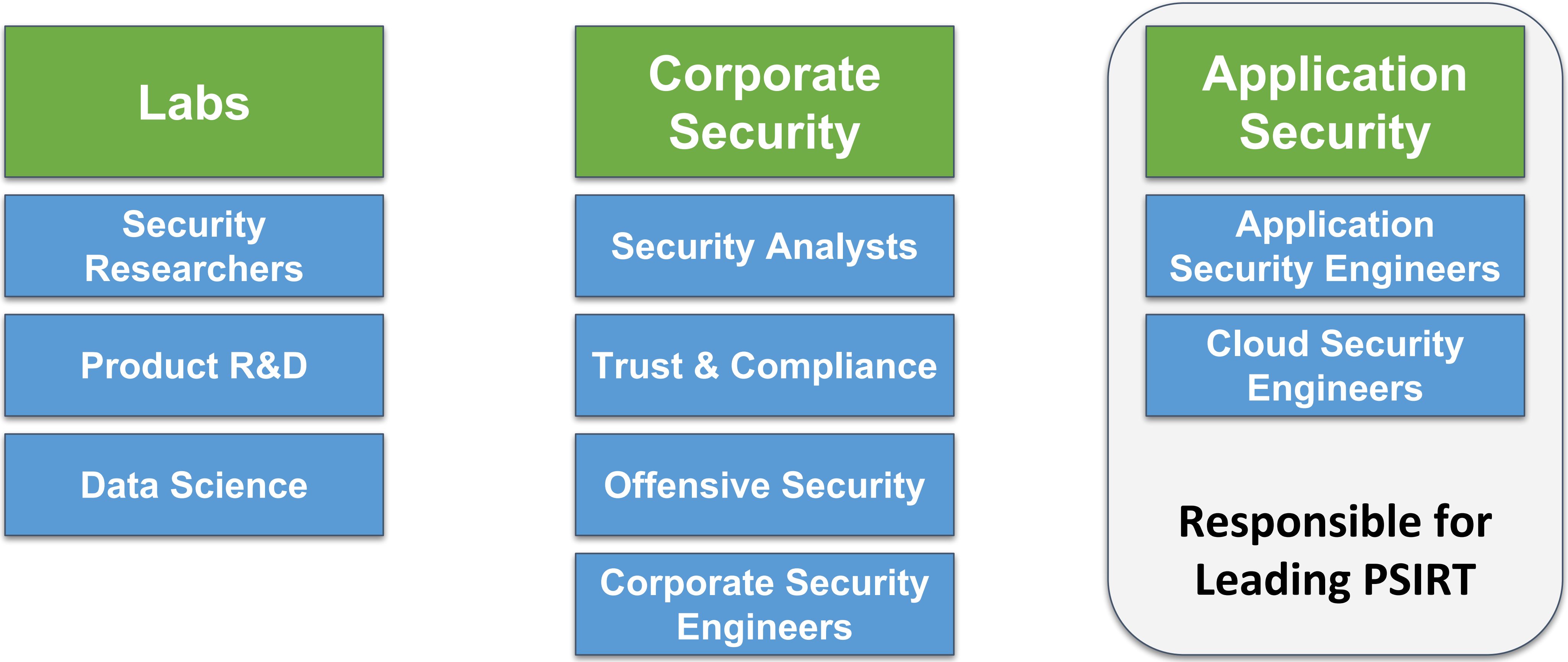
Focuses Since the Beginning...

- Bugs happen. How you respond is (usually) what counts most.
- Be transparent to customers.
- Index on the fast remediation & communication of critical issues.
- Be appreciative of researchers.

Framing Our Organization

- **Established:** 2010
- **Customers:** 10,000+
- **Employees:** 600+
- **Focus:** SaaS Authentication & End-point Security Technologies.

Our Overall Security Organization



Labs

- Security Researchers
- Product R&D
- Data Science

Corporate Security

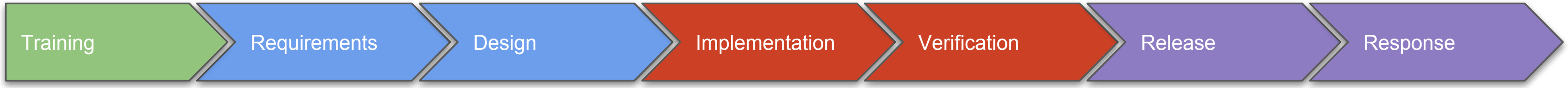
- Security Analysts
- Trust & Compliance
- Offensive Security
- Corporate Security Engineers

Application Security

- Application Security Engineers
- Cloud Security Engineers

Responsible for Leading PSIRT

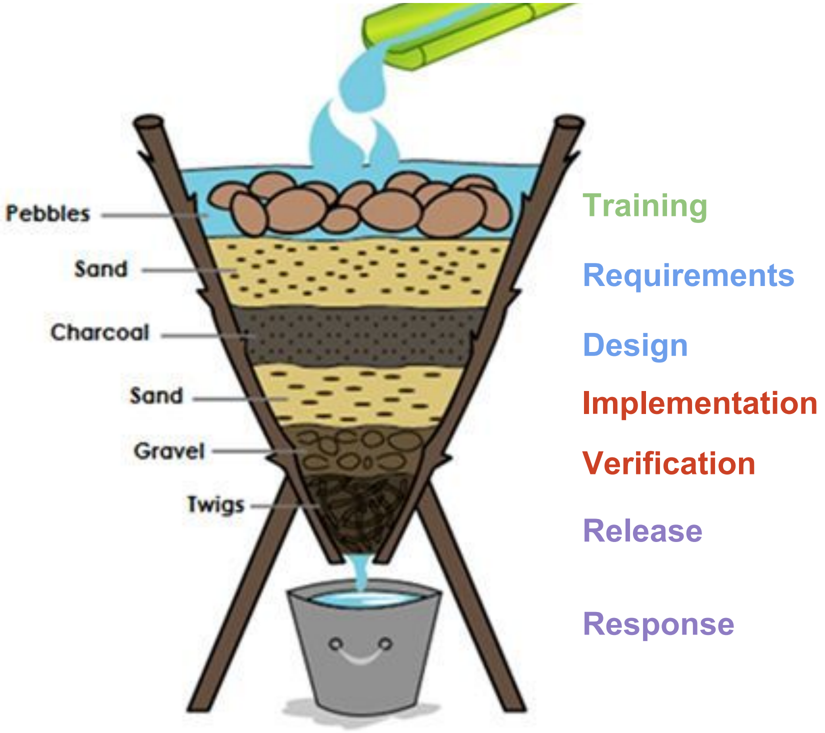
Security Development Lifecycle (SDL)



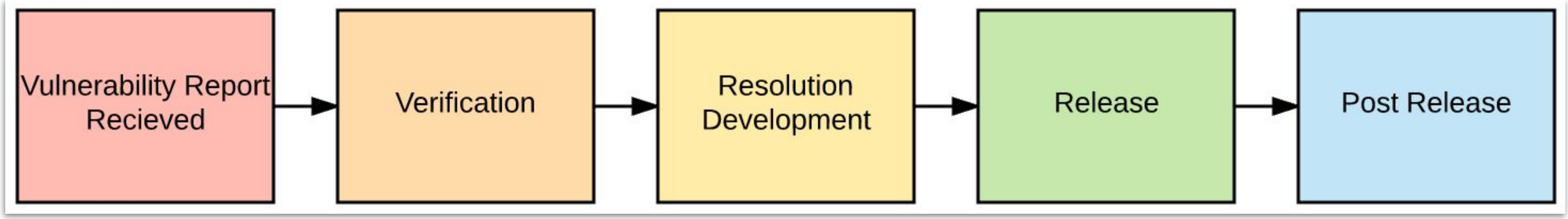
- We map offered team “services” against the SDL to support Engineers throughout the entire SDLC.

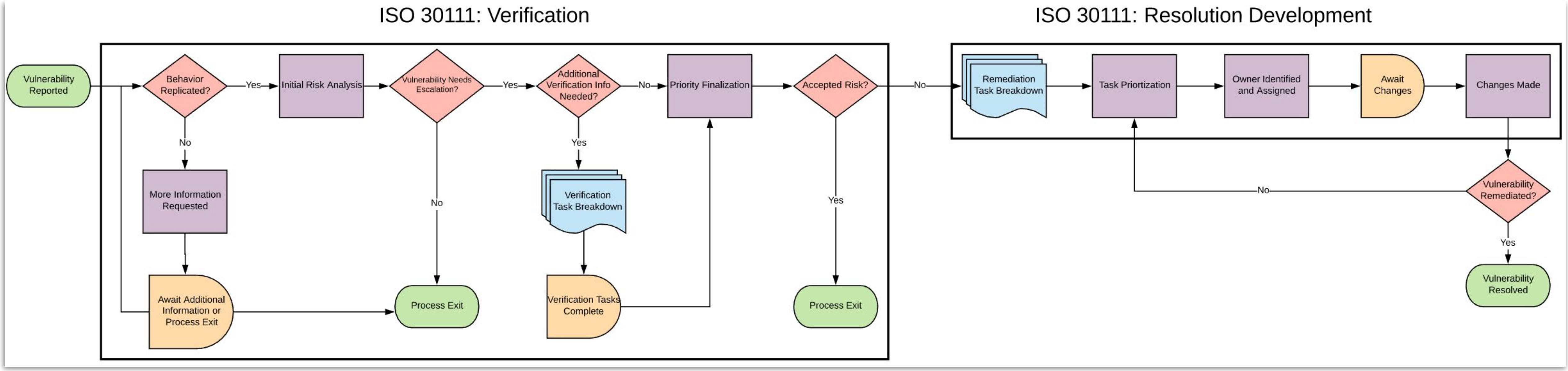
- Response is something we want to be great at, but work hard throughout the entire SDL to minimize the need.

- We invest early, and often, in security.



Security Defect Handling



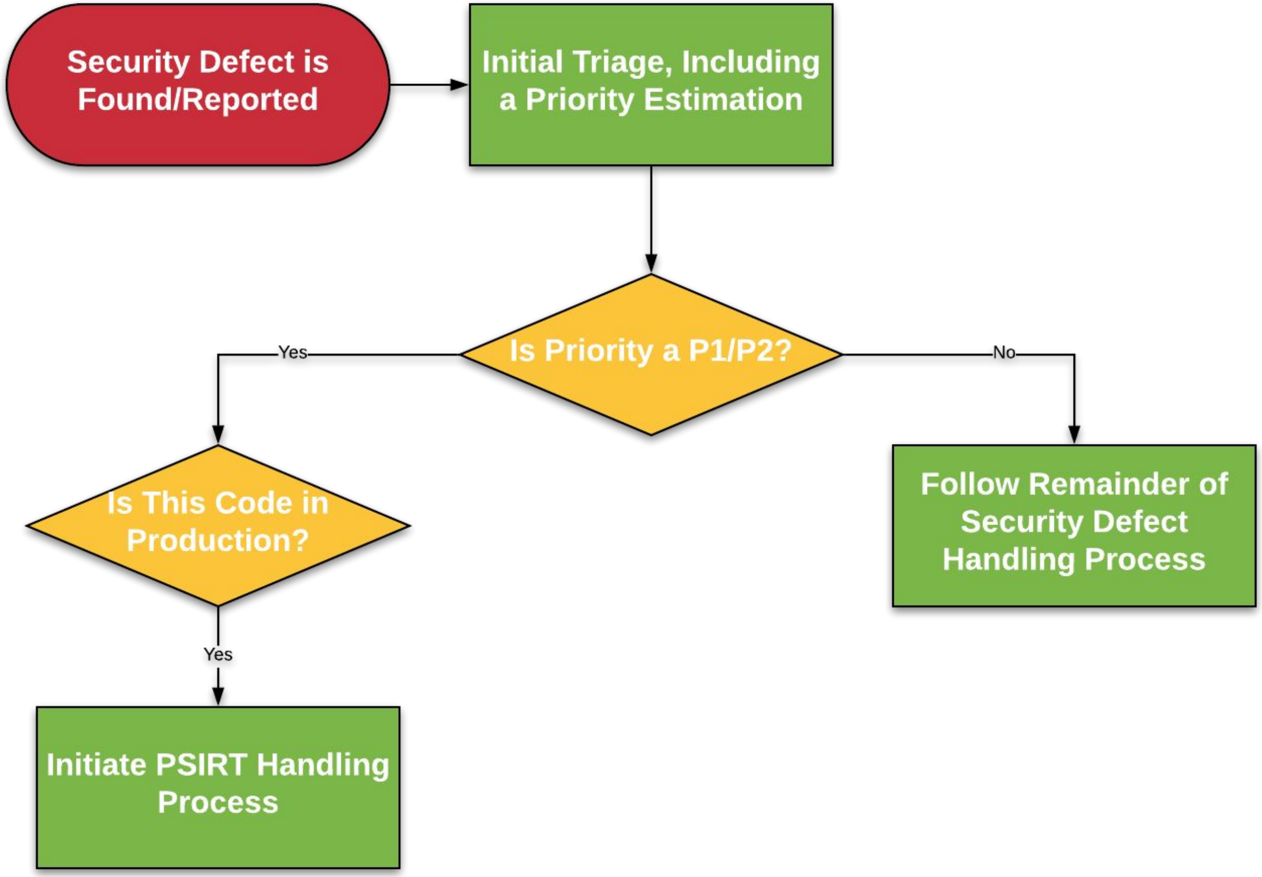


ISO 30111: Verification
ISO 30111: Resolution Development
Vulnerability Reported
Behavior Replicated?
Yes
No
Initial Risk Analysis
Vulnerability Needs Escalation?
Yes
No
Additional Verification Info Needed?
No
Yes
Priority Finalization
Accepted Risk?
No
Yes
More Information Requested
Await Additional Information or Process Exit
Process Exit
Verification Task Breakdown
Verification Tasks Complete
Process Exit
Remediation Task Breakdown
Task Priortization
Owner Identified and Assigned
Await Changes
Changes Made
Vulnerability Remediated?
No
Yes
Vulnerability Resolved

Initiation of PSIRT Incident Handling Process

- Any Critical or High security defect found in our production services or released software is likely to initiate a PSIRT incident.

- The Application Security team operates with discretion and brings in stakeholders to support the process when most relevant.


Security Defect is Found/Reported

Initial Triage, Including a Priority Estimation

Is Priority a P1/P2?

Yes

No

Is This Code in Production?

Follow Remainder of Security Defect Handling Process

Yes

Initiate PSIRT Handling Process

Stakeholders to Execute Successful Response

- **Application Security:** Initiation & Management of the PSIRT Process.
- **Customer Success:** Ensures That All Customers Can Remediate Issues.
- **Marketing:** Provides Email & Social Media Outreach to Our Customers.
- **Engineering Operations:** Deploys Fixes to Our Cloud Service.
- **Legal:** Aligns Our Response to the Needs of Contractual Obligations.
- **PR:** Supports Drafting of All Communications for Outreach.
- **Engineering:** Creates Necessary Patches to Remediate Defects.
- **Quality Assurance:** Tests Patches to Limit Software Regressions.

Our PSIRT Execution Template

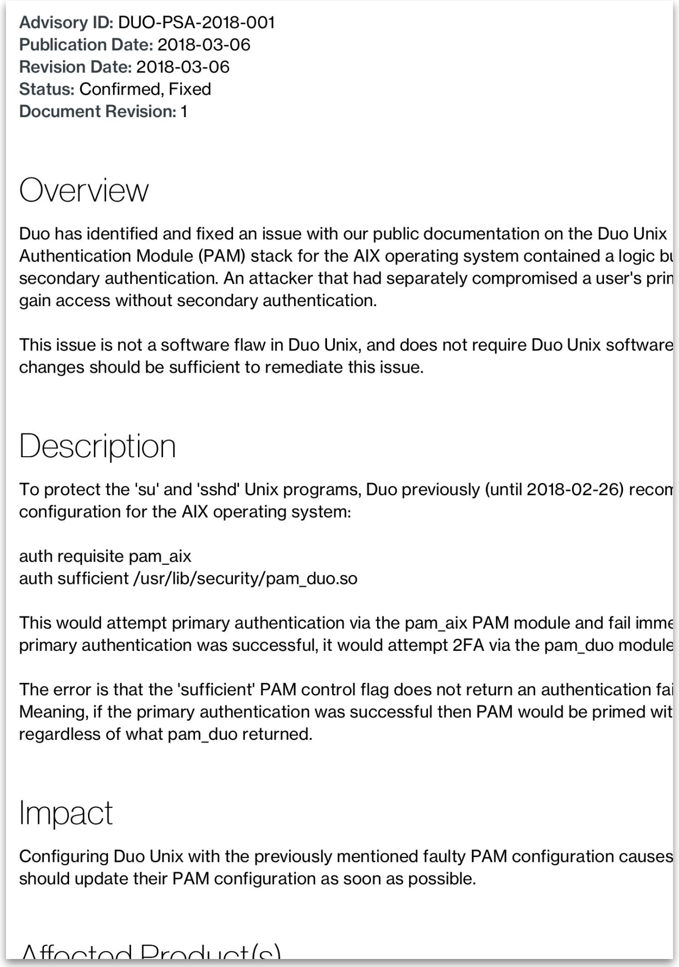
- **Initial Report** (Who? When? Via What Method?)
- **List of PSIRT Stakeholders** (Who? Role?)
- **Advisory Publication** (When? Where?)
- **Security Metrics & Scores** (CVSS, CWE, VRT)
- **Reproduction Details** (Who? When? How?)
- **Remediation Tracking** (Patch Links with Description)
- **Issue Overview** (Summary, Root Cause, Impact, Resolution)
- **Timeline** (Date & Time for All Major Events/Actions Taken)
- **Workflow Checklist** (Sign-off with Name & Date for Each Step)
- **Meeting Notes** (When? Who? Where? Duration? Notes & Actions)
- **Post Mortem** (Who? When? Details for Each Q & A Focus)

Outreach - Product Security Advisory (PSA)

Context: Generally used for 'Critical' (P1) security defects. May, or may not, have action required by customers to resolve. Large focus on customers having useful information to make decisions with.

Method(s):

- GPG-signed email to impacted customers.
- All PSAs are added to our public web site.
- Additional outreach may occur 1:1 via phone.
- May result in blog post for additional depth.



Advisory ID: DUO-PSA-2018-001
Publication Date: 2018-03-06
Revision Date: 2018-03-06
Status: Confirmed, Fixed
Document Revision: 1

Overview

Duo has identified and fixed an issue with our public documentation on the Duo Unix Authentication Module (PAM) stack for the AIX operating system contained a logic bu secondary authentication. An attacker that had separately compromised a user's prin gain access without secondary authentication.

This issue is not a software flaw in Duo Unix, and does not require Duo Unix software changes should be sufficient to remediate this issue.

Description

To protect the 'su' and 'sshd' Unix programs, Duo previously (until 2018-02-26) recom configuration for the AIX operating system:

auth requisite pam_aix
auth sufficient /usr/lib/security/pam_duo.so

This would attempt primary authentication via the pam_aix PAM module and fail imme primary authentication was successful, it would attempt 2FA via the pam_duo module

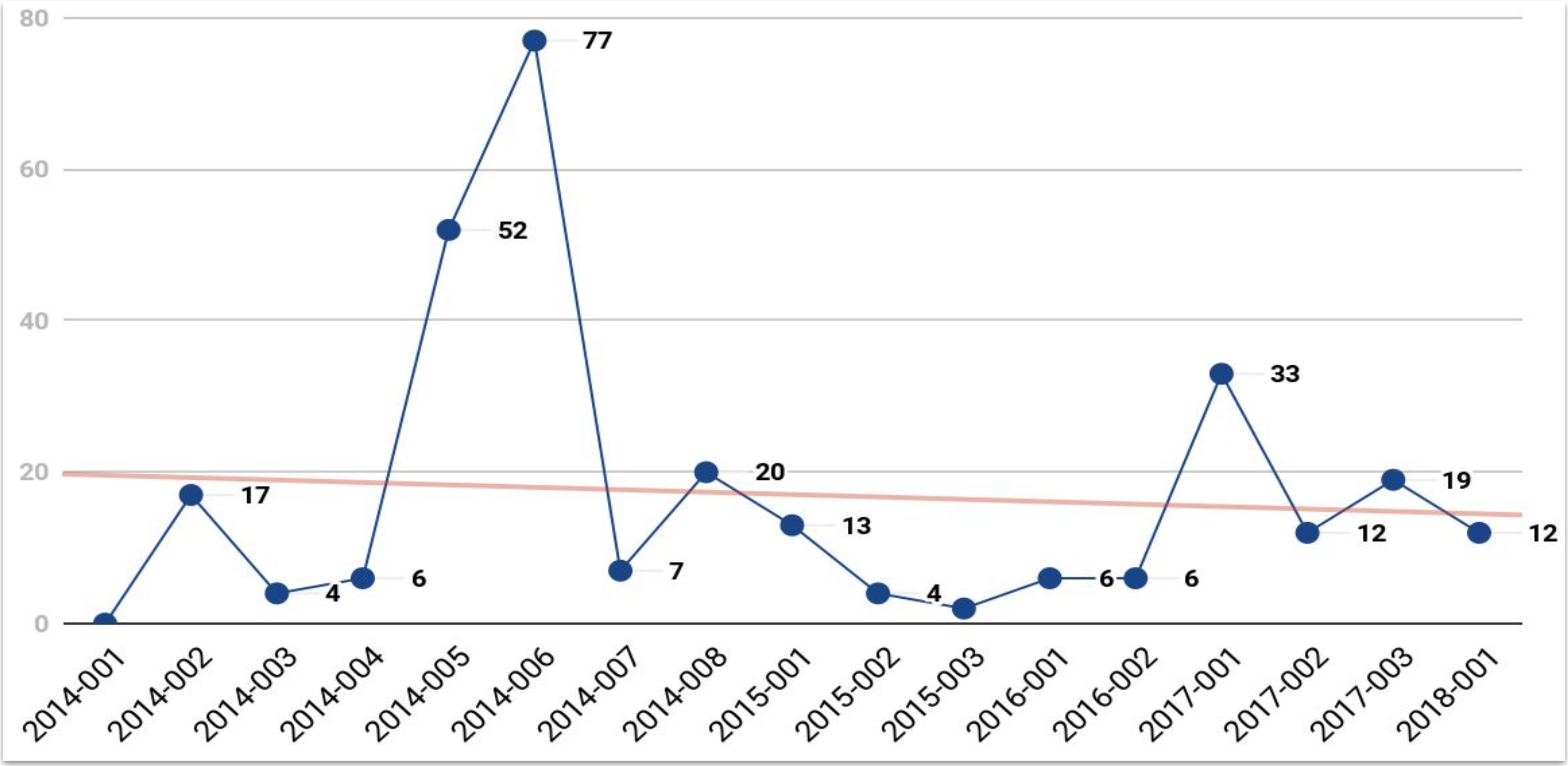
The error is that the 'sufficient' PAM control flag does not return an authentication fai Meaning, if the primary authentication was successful then PAM would be primed wit regardless of what pam_duo returned.

Impact

Configuring Duo Unix with the previously mentioned faulty PAM configuration causes should update their PAM configuration as soon as possible.

Affected Product(s)

Days From Discovery to Customer Receiving PSA



There Were a Few Missteps Along the Way

PSIRT Outtake #1 (2014)

Emailing our first Product Security Advisory as a PDF. We had a few customers asking if we were sending them malware. *facepalm*

PSIRT Outtake #2 (2014)

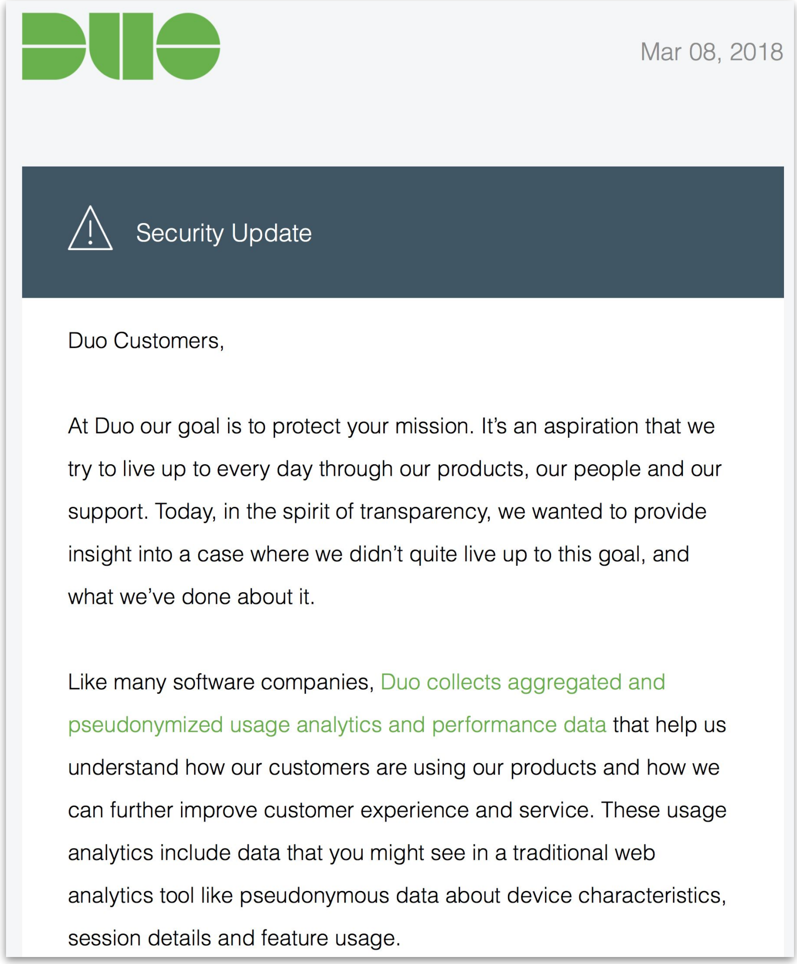
We released a PSA before the fix was even ready, causing a bit of chaos...

Outreach - Customer Notification

Context: For non-Critical security & privacy issues, we provide customers with more narrative details of a concern they should know about with clear, transparent communication being our top priority.

Method(s):

- Email is sent to all impacted customers.
- May be posted as a blog for wider accessibility.
- Additional outreach may occur 1:1 via phone.



Mar 08, 2018

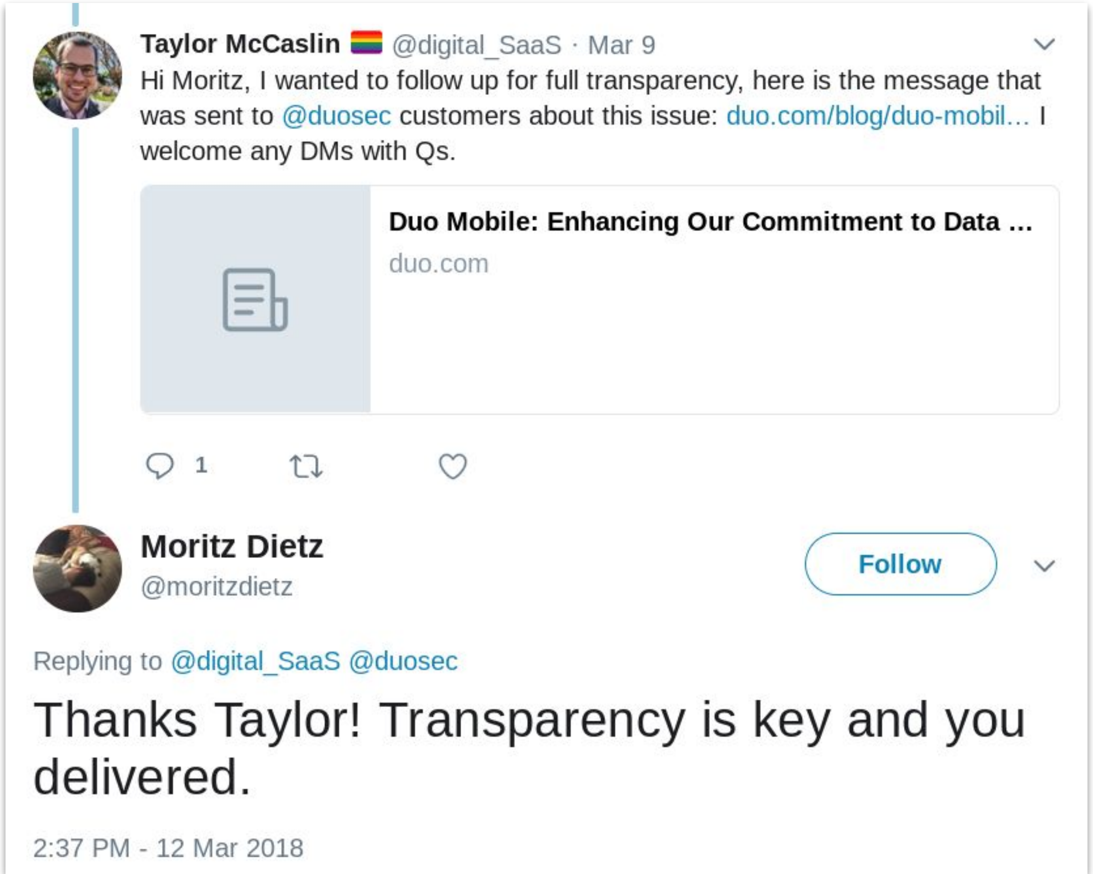
⚠ Security Update

Duo Customers,

At Duo our goal is to protect your mission. It's an aspiration that we try to live up to every day through our products, our people and our support. Today, in the spirit of transparency, we wanted to provide insight into a case where we didn't quite live up to this goal, and what we've done about it.

Like many software companies, Duo collects aggregated and pseudonymized usage analytics and performance data that help us understand how our customers are using our products and how we can further improve customer experience and service. These usage analytics include data that you might see in a traditional web analytics tool like pseudonymous data about device characteristics, session details and feature usage.

Customers Value When Companies Proactively Do the Right Thing...



Taylor McCaslin 🏳️‍🌈 @digital_SaaS · Mar 9

Hi Moritz, I wanted to follow up for full transparency, here is the message that was sent to @duosec customers about this issue: duo.com/blog/duo-mobil… I welcome any DMs with Qs.

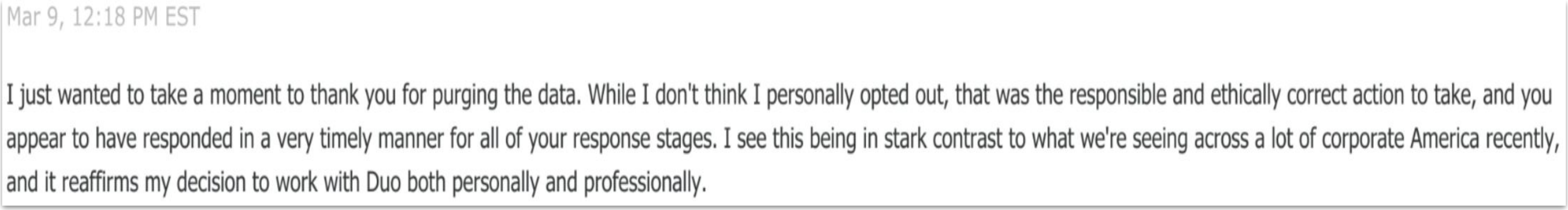
Duo Mobile: Enhancing Our Commitment to Data …
duo.com

Moritz Dietz
@moritzdietz

Replying to @digital_SaaS @duosec

Thanks Taylor! Transparency is key and you delivered.

2:37 PM - 12 Mar 2018



Mar 9, 12:18 PM EST

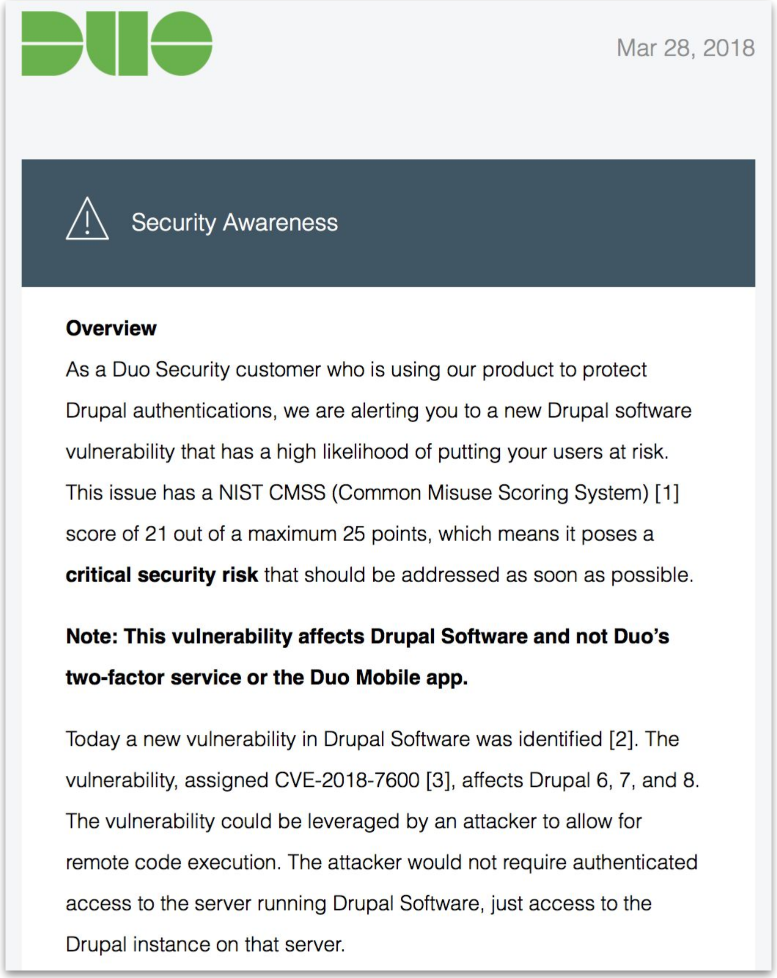
I just wanted to take a moment to thank you for purging the data. While I don't think I personally opted out, that was the responsible and ethically correct action to take, and you appear to have responded in a very timely manner for all of your response stages. I see this being in stark contrast to what we're seeing across a lot of corporate America recently, and it reaffirms my decision to work with Duo both personally and professionally.

Outreach - Threat Notification

Context: To provide customers awareness that a technology we believe they use has a security issue outside of the direct context of our product.

Method(s):

- Email is sent to all likely relevant customers.
- Additional outreach may occur 1:1 via phone.



Mar 28, 2018

⚠ Security Awareness

Overview

As a Duo Security customer who is using our product to protect Drupal authentications, we are alerting you to a new Drupal software vulnerability that has a high likelihood of putting your users at risk. This issue has a NIST CMSS (Common Misuse Scoring System) [1] score of 21 out of a maximum 25 points, which means it poses a **critical security risk** that should be addressed as soon as possible.

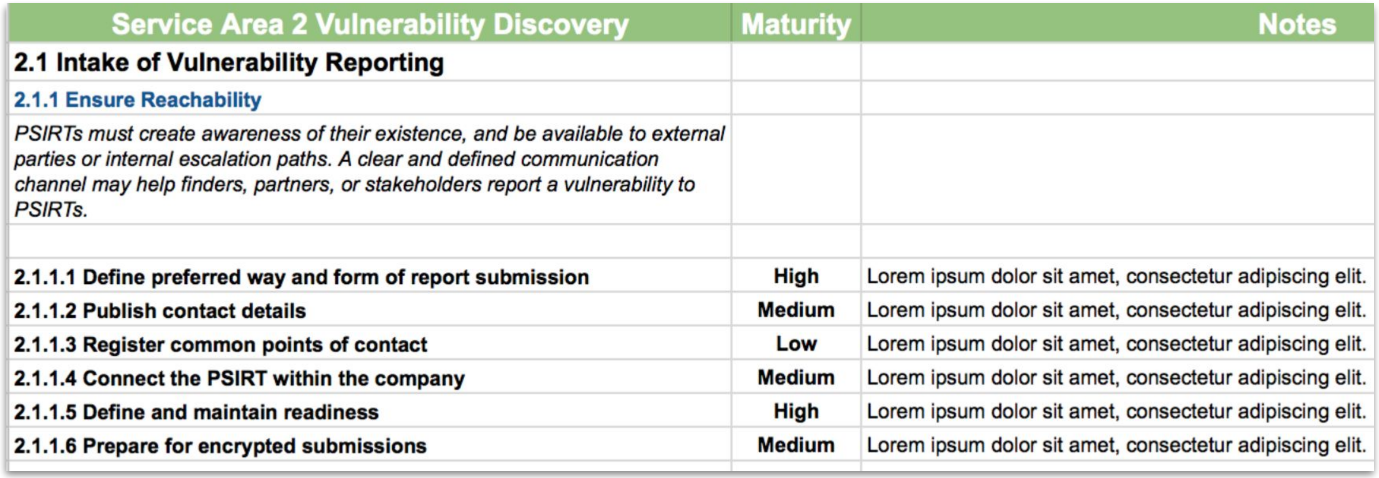
Note: This vulnerability affects Drupal Software and not Duo's two-factor service or the Duo Mobile app.

Today a new vulnerability in Drupal Software was identified [2]. The vulnerability, assigned CVE-2018-7600 [3], affects Drupal 6, 7, and 8. The vulnerability could be leveraged by an attacker to allow for remote code execution. The attacker would not require authenticated access to the server running Drupal Software, just access to the Drupal instance on that server.

Improving Our Program's Depth & Breadth

- Created a good-enough draft spreadsheet of the Framework for an internal gap analysis.
- Frameworks are not checklists, but they can definitely help to structurally review your efforts.
- Also a great way to consider new ideas or revisit old ones.

We Measured & Annotated **195** Facets of Our PSIRT in Their Current State!

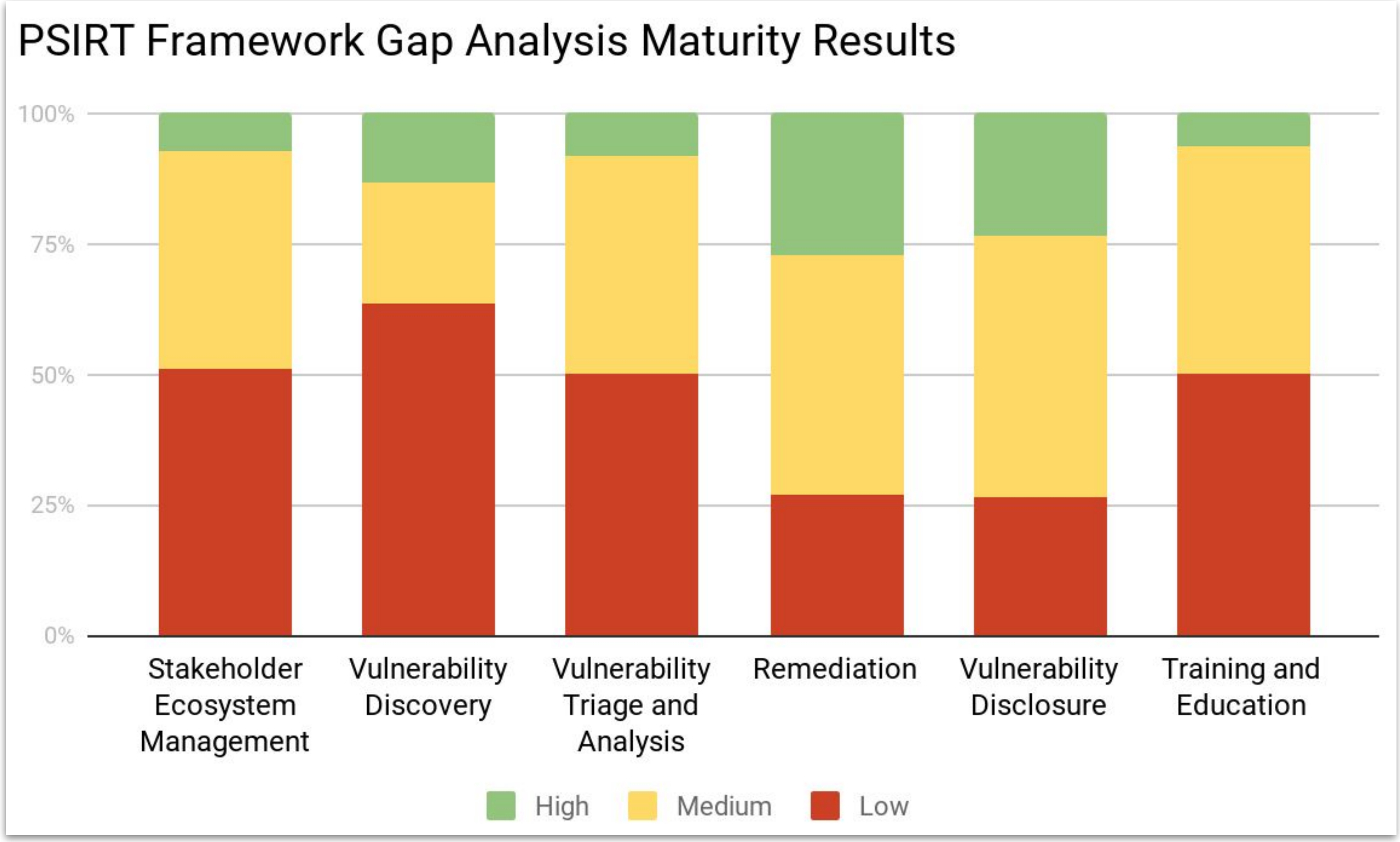


Service Area 2 Vulnerability Discovery	Maturity	Notes
2.1 Intake of Vulnerability Reporting		
2.1.1 Ensure Reachability		
PSIRTs must create awareness of their existence, and be available to external parties or internal escalation paths. A clear and defined communication channel may help finders, partners, or stakeholders report a vulnerability to PSIRTs.		
2.1.1.1 Define preferred way and form of report submission	**High**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2.1.1.2 Publish contact details	**Medium**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2.1.1.3 Register common points of contact	**Low**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2.1.1.4 Connect the PSIRT within the company	**Medium**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2.1.1.5 Define and maintain readiness	**High**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2.1.1.6 Prepare for encrypted submissions	**Medium**	Lorem ipsum dolor sit amet, consectetur adipiscing elit.

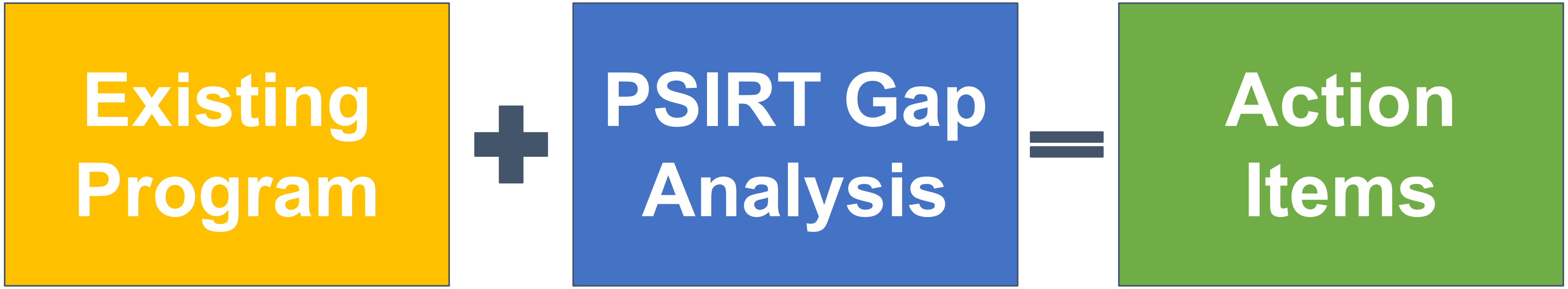
*** why yes, that is fake data! :)**

Considering Our Aggregated Results (Dec. 2017)

- Reflects a conservative view for each facet to prevent us from lying to ourselves :)
- Helped to frame with more specificity the perceptions we had of our own program.
- Provided a crucial "input" to our next-step planning...

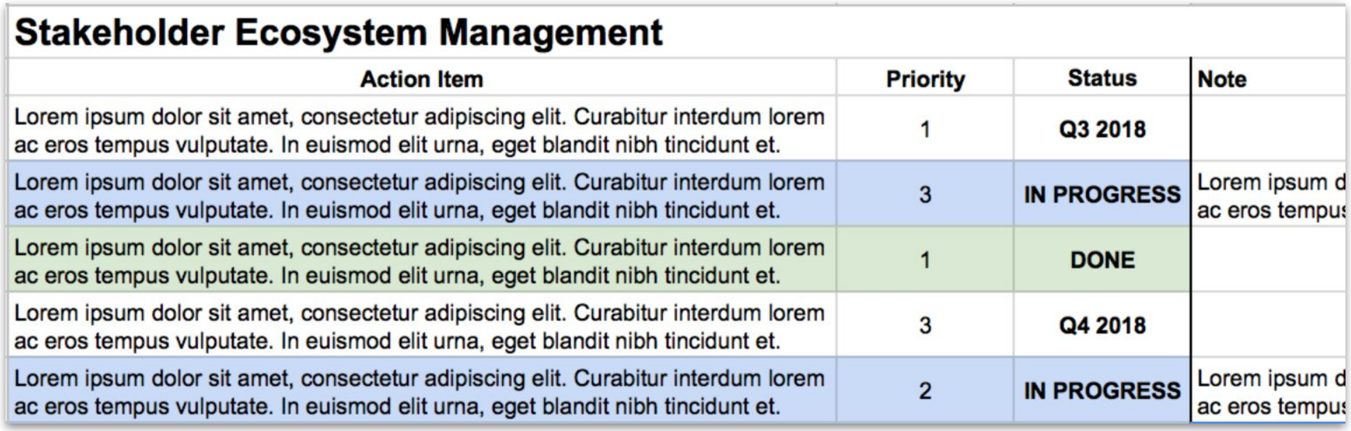


Now What? More Spreadsheets, Duh!



Existing Program + PSIRT Gap Analysis = Action Items

1. Identify themes within areas
2. Define program enhancements
3. Assign a priority and timeline
4. Execute!



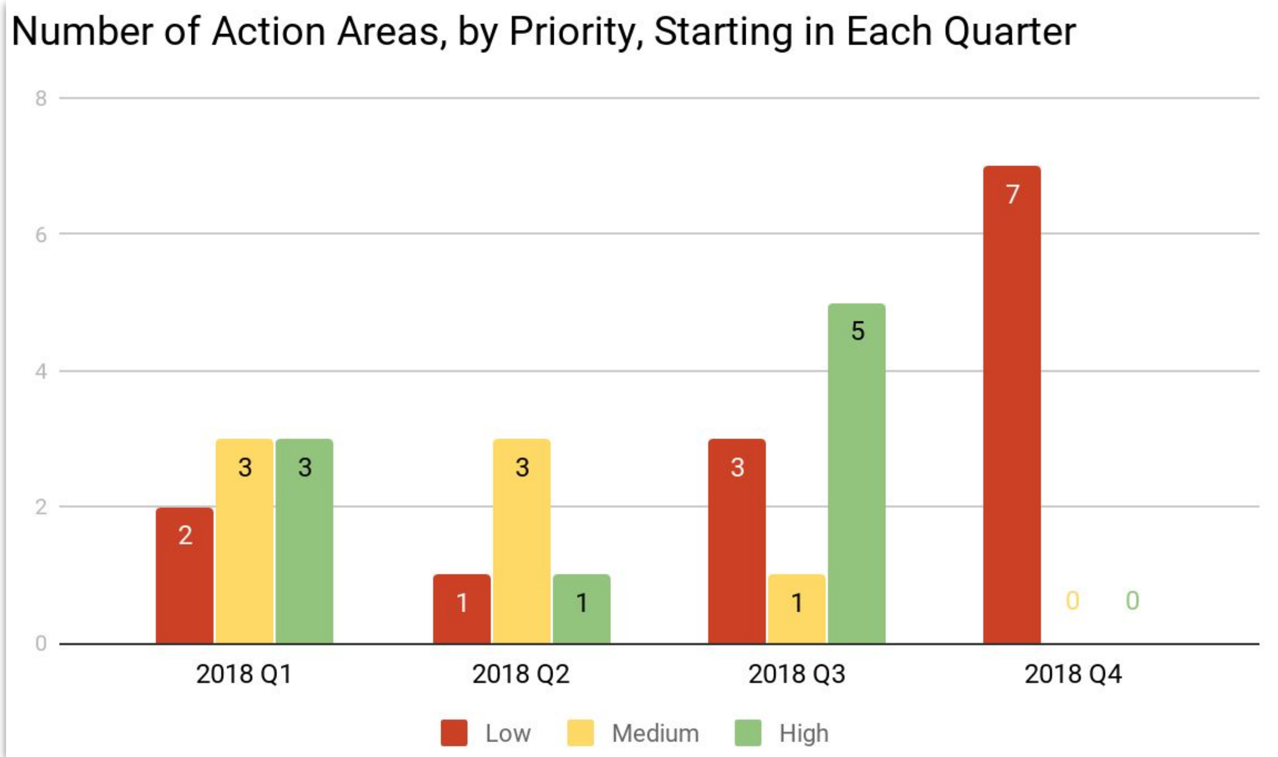
Stakeholder Ecosystem Management

Action Item	Priority	Status	Note
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempus vulputate. In euismod elit urna, eget blandit nibh tincidunt et.	1	Q3 2018	
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempus vulputate. In euismod elit urna, eget blandit nibh tincidunt et.	3	IN PROGRESS	Lorem ipsum d ac eros tempus
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempus vulputate. In euismod elit urna, eget blandit nibh tincidunt et.	1	DONE	
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempus vulputate. In euismod elit urna, eget blandit nibh tincidunt et.	3	Q4 2018	
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempus vulputate. In euismod elit urna, eget blandit nibh tincidunt et.	2	IN PROGRESS	Lorem ipsum d ac eros tempus

*** why yes, that is fake data! :)**

PSIRT Enhancement Breakdown

- 29 “action areas,” that each may have a few tactical items a piece.
- Quarterly planning with the intent to resolve all action areas within 2018, considerate of dependencies.
- At end of year, re-measure against the non-draft(?) PSIRT Framework.



Example Program Gaps & Resulting Action Items

Focus Area: *Incident Post-mortem process* (1.1.3)

Gap Note: *“A post-mortem may happen for a severe enough issue, but not regimented or well structured.”*

Enhancement:

- Established a mandatory post-mortem process to be done within a week following the resolution of an incident.
- Formalized a section of our “PSIRT Execution Template” to put those details in the same file for long-term alignment.

Example Program Gaps & Resulting Action Items

Focus Area: *Handle Vulnerability Reports (2.1.2)*

Gap Note: *“Published SLA on disclosure page, but adherence to that by PSIRT needs better process & handling in place.”*

Enhancement:

- Created an “External Security Response” process that uses per-stage SLA timelines to ensure we always act promptly.
- Leveraged ISO 30111 (Vulnerability Handling Processes) to align our program with industry standards for our actions.

Example Program Gaps & Resulting Action Items

Focus Area: *Collect data (3.1.2.1) & Finder Profile (3.2.3)*

Gap Note: *"Establish a location to collect details about the people who submit vulnerabilities to us. This could include bug reports historically, contact details, quality metrics, etc."*

Enhancement:

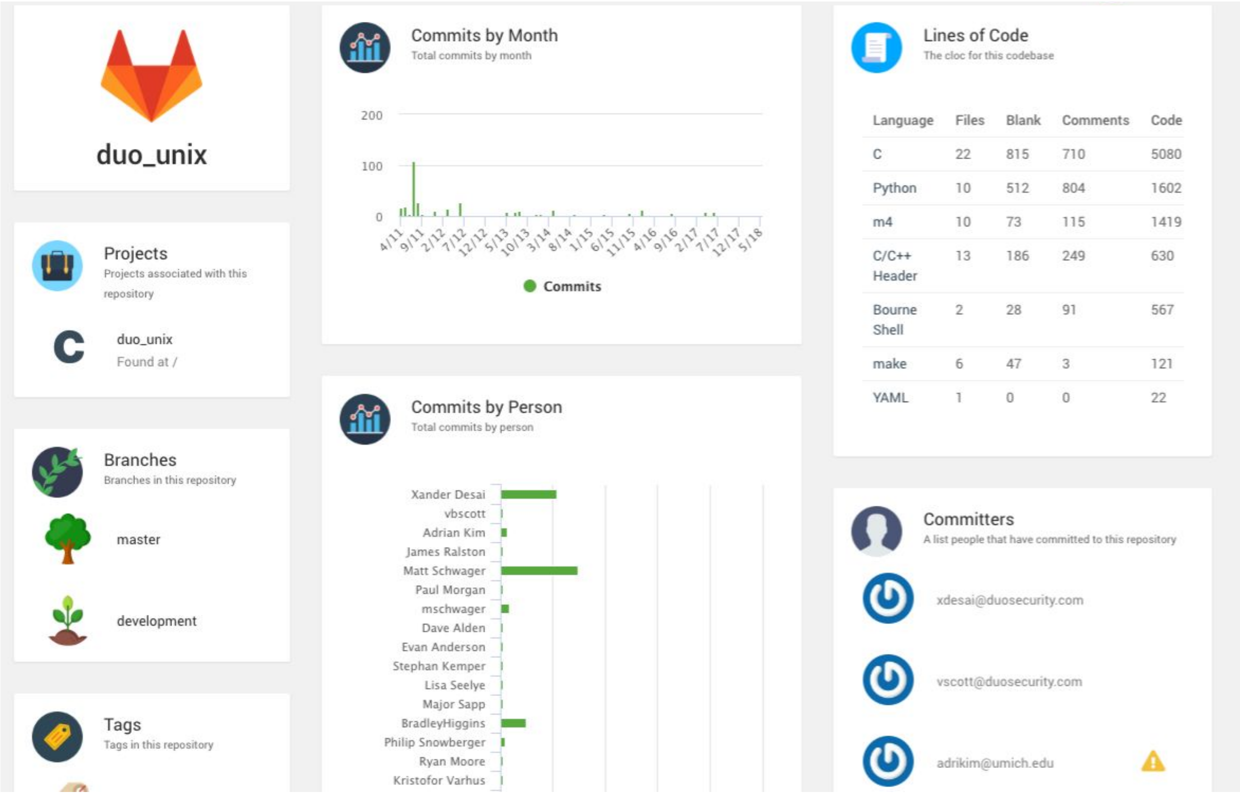
- Tracking metadata about all "External Security Response" actions we take to more fully understand our reporters.
- Retroactively went back a year to populate information of people who contacted us prior to establishing this data set.

Key Themes for Enhancements in 2018

- **Document:** Define comprehensive workflows for PSIRT incidents, train stakeholders, update processes, and execute a full PSIRT drill.
- **Inventory:** Build & procure technologies that provide a detailed view of software security, writ large, to fully understand our PSIRT scope.
- **Communicate:** Improve internal communicate methodologies during PSIRT incidents and update our web site's content for third-parties.
- **Measure:** Track adherence to internal SLAs for both defect resolution & external security response engagement. Establish PSIRT KPIs.

Security Software Inventory (SSI)

- 100% in-house developed to be a single pane of glass for our holistic view of software security at Duo.
- Leverages an aggregation of the auto-discovered repositories from many locations across our company.
- Ultimately will provide a singular portal for day-to-day AppSec needs.



duo_unix

Projects
Projects associated with this repository

duo_unix
Found at /

Branches
Branches in this repository

master

development

Tags
Tags in this repository

Commits by Month
Total commits by month

Commits by Person
Total commits by person

Lines of Code
The cloc for this codebase

Language	Files	Blank	Comments	Code
C	22	815	710	5080
Python	10	512	804	1602
m4	10	73	115	1419
C/C++ Header	13	186	249	630
Bourne Shell	2	28	91	567
make	6	47	3	121
YAML	1	0	0	22

Committers
A list people that have committed to this repository

xdesai@duosecurity.com

vscott@duosecurity.com

adrikim@umich.edu ⚠

Tips For Successful a PSIRT

- **Provide a Large “Front Door” to Finders**
  - Publish PSIRT contact details on your web site.
  - Provide a GPG key for secure communications.
- **Release “Bad News” on Tuesday - Thursday**
  - Don’t bury your bugs under weekends/holidays.
  - The quickest way to make critics is via poor timing.
- **Keep the PSIRT Strategic *and* Technical**
  - A great PSIRT must be able to understand technical security defects to be an effective partner with teams.
  - ...but you need decisive, organized leadership, too!

Key Takeaways

1. While PSIRT representation is skewed towards larger enterprises, it’s much easier to build a product security program while you’re small.
2. Whether customers, security researchers, or internal employees, do not forget that being polite, prompt, and transparent go a *long* way.
3. Don’t try to do it all. Use the PSIRT Framework as a jumping-off point to align your PSIRT effort to the needs of the business & customers.
4. Invest your time wisely ahead of incidents to save time during them.

30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

Thank you!
Questions?

Mark Stanislav

mstanislav@duo.com

FIRST™
Improving Security Together