Crawl, Walk, Run: Living the PSIRT Framework

Mark Stanislav
Director of Application Security, Duo Security
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!
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.
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

- Behavior Replicated?
  - Yes: Initial Risk Analysis
  - No: More Information Requested
    - Yes: Await Additional Information or Process Exit
    - No: Process Exit

ISO 30111: Resolution Development

- Vulnerability Remediated?
  - Yes: Vulnerability Resolved
  - No: Process Exit

- Verification Task Breakdown?
  - Yes: Verification Tasks Complete
  - No: Process Exit

- Task Prioritization?
  - Yes: Owner Identified and Assigned
  - No: Process Exit

- Asset Changes?
  - Yes: Changes Made
  - No: Process Exit

- Verification Needed?
  - Yes: Verification Tasks Complete
  - No: Process Exit

- Priority Finalized?
  - Yes: Accepted Risk?
  - No: Process Exit
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.
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.
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.
Customers Value When Companies Proactively Do the Right Thing...

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.
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!

* why yes, that is fake data! :)

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

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

<table>
<thead>
<tr>
<th>Stakeholder Ecosystem Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Item</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempor vulputate. In euismod elit urma, eget blandit nibh tincidunt et.</td>
</tr>
<tr>
<td>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempor vulputate. In euismod elit urma, eget blandit nibh tincidunt et.</td>
</tr>
<tr>
<td>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempor vulputate. In euismod elit urma, eget blandit nibh tincidunt et.</td>
</tr>
<tr>
<td>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur interdum lorem ac eros tempor vulputate. In euismod elit urma, eget blandit nibh tincidunt et.</td>
</tr>
</tbody>
</table>

* why yes, that is fake data! :)

Existing Program + PSIRT Gap Analysis = Action Items
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.

![Number of Action Areas, by Priority, Starting in Each Quarter]

- Low
- Medium
- High
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.
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.
Thank you!
Questions?

Mark Stanislav
mstanislav@duo.com