# Daily Challenges for Synology PSIRT.

Synolgoy Mike Jiang

Synology®

# Who is Synology ?

Synology

# Synology Inc.

- Founded in 2000
- NAS

Synology


Synology

# What is NAS?

# Network Attached Storage

Synology

# Network Application Storage

Synology

# Synology Products

- Hardware: NAS, Router, Surveillance

# Synology Products

- Hardware: NAS, Router, Surveillance
- OS: DSM, SRM, VS960HD

Synology

# Synology Products

- Hardware: NAS, Router, Surveillance
- OS: DSM, SRM, VS960HD
- Packages: Multemedia, Collaboration, Web

# Synology Products

- Hardware: NAS, Router, Surveillance
- OS: DSM, SRM, VS960HD
- Packages: Multemedia, Collaboration
- Mobile and Desktop Application

# Synology Products

- Hardware: NAS, Router, Surveillance
- OS: DSM, SRM, VS960HD
- Packages: Multemedia, Collaboration
- Mobile and Desktop Application

# Agenda

- Synology PSIRT
- Synology PSIRT Framework
- Security Organization
- Bounty Program

Synology

沒有絕對安全的產品，
我們能做的是當事件發生時盡快修復。

Synology

# Synology PSIRT

Synology

```
473      */
474     bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
475     {
476             NTSTATUS status;
477
478             if (lp_disable_spoolss() && strequal(pipename, "spoolss")) {
479                     DEBUG(10, ("refusing spoolss access\n"));
480                     return false;
481             }
482
483             if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
484                     return true;
485             }
486
487             status = smb_probe_module("rpc", pipename);
488             if (!NT_STATUS_IS_OK(status)) {
489                     DEBUG(10, ("is_known_pipename: %s unknown\n", pipename));
490                     return false;
491             }
492             DEBUG(10, ("is_known_pipename: %s loaded dynamically\n", pipename));
493
494             /*
495              * Scan the list again for the interface id
496              */
497             if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
```

SAMBACRY

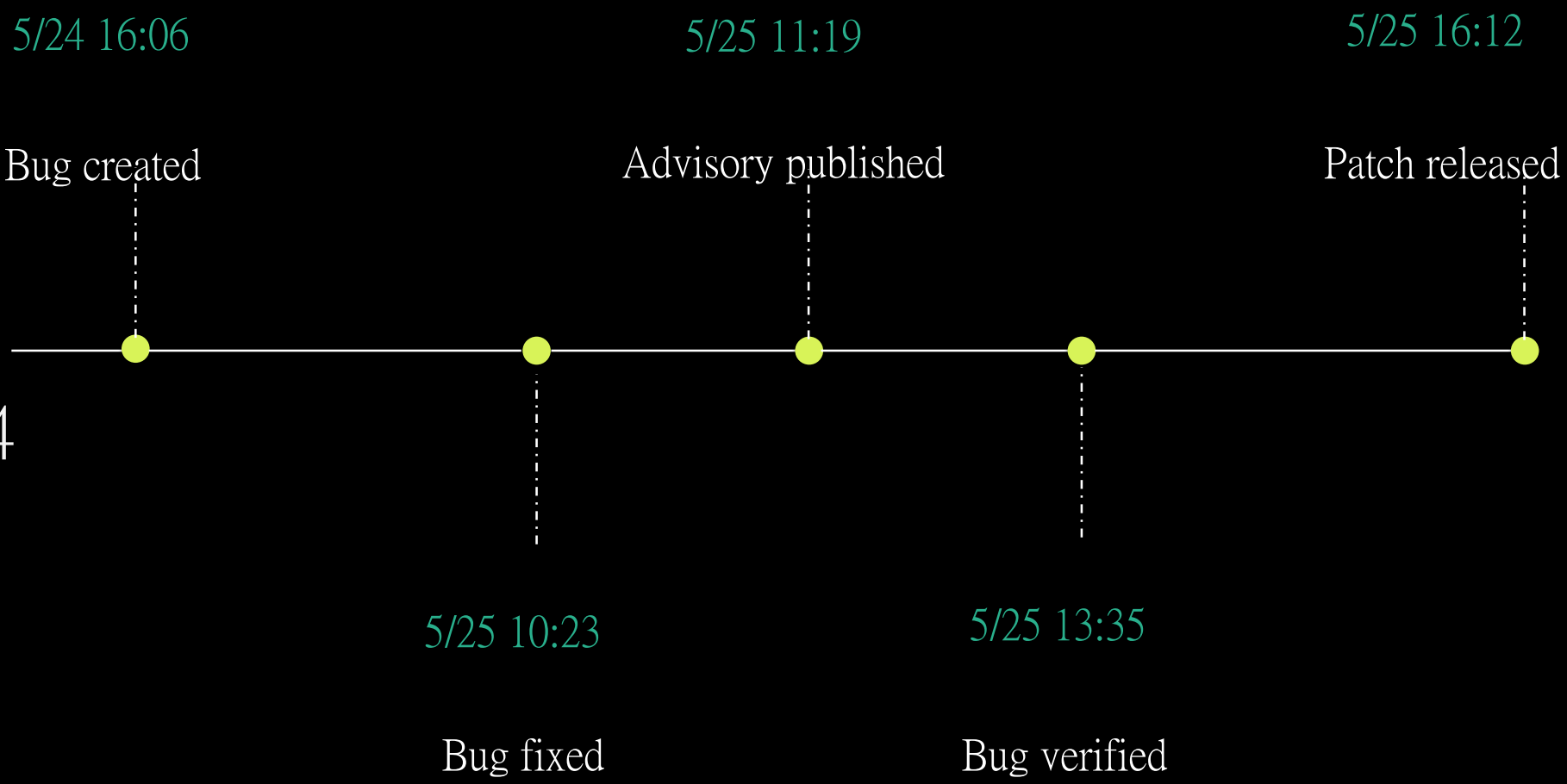
CVE-2017-7494

Synology

DSM

# SambaCry

## CVE-2017-7494




Synology

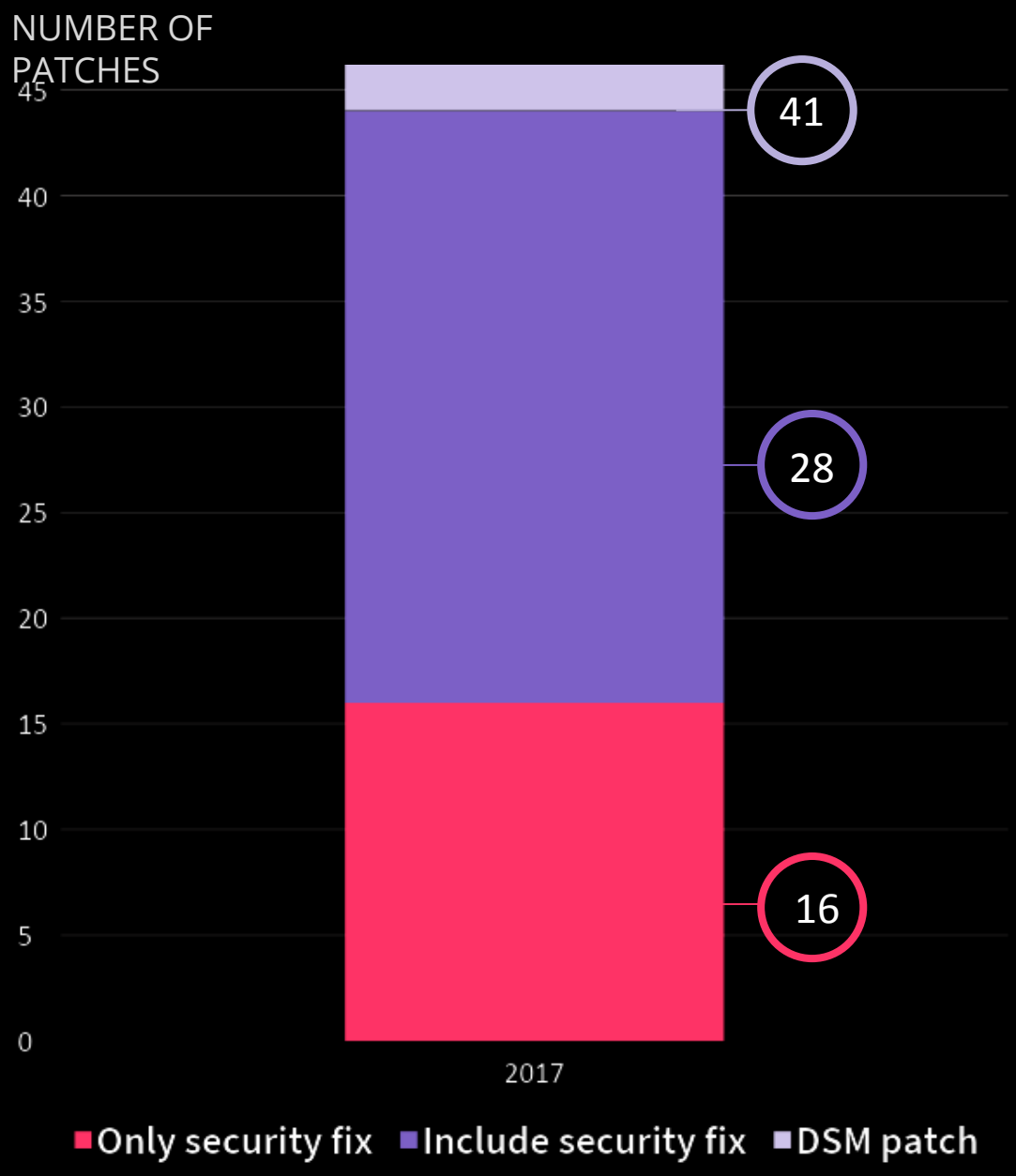
# Fast Incident Response

- HeartBleed for 48 hours
- Sambacry for 24 hours
- CVE-2017-14491 for 24 hours
- Krack for 24 hours

Synology

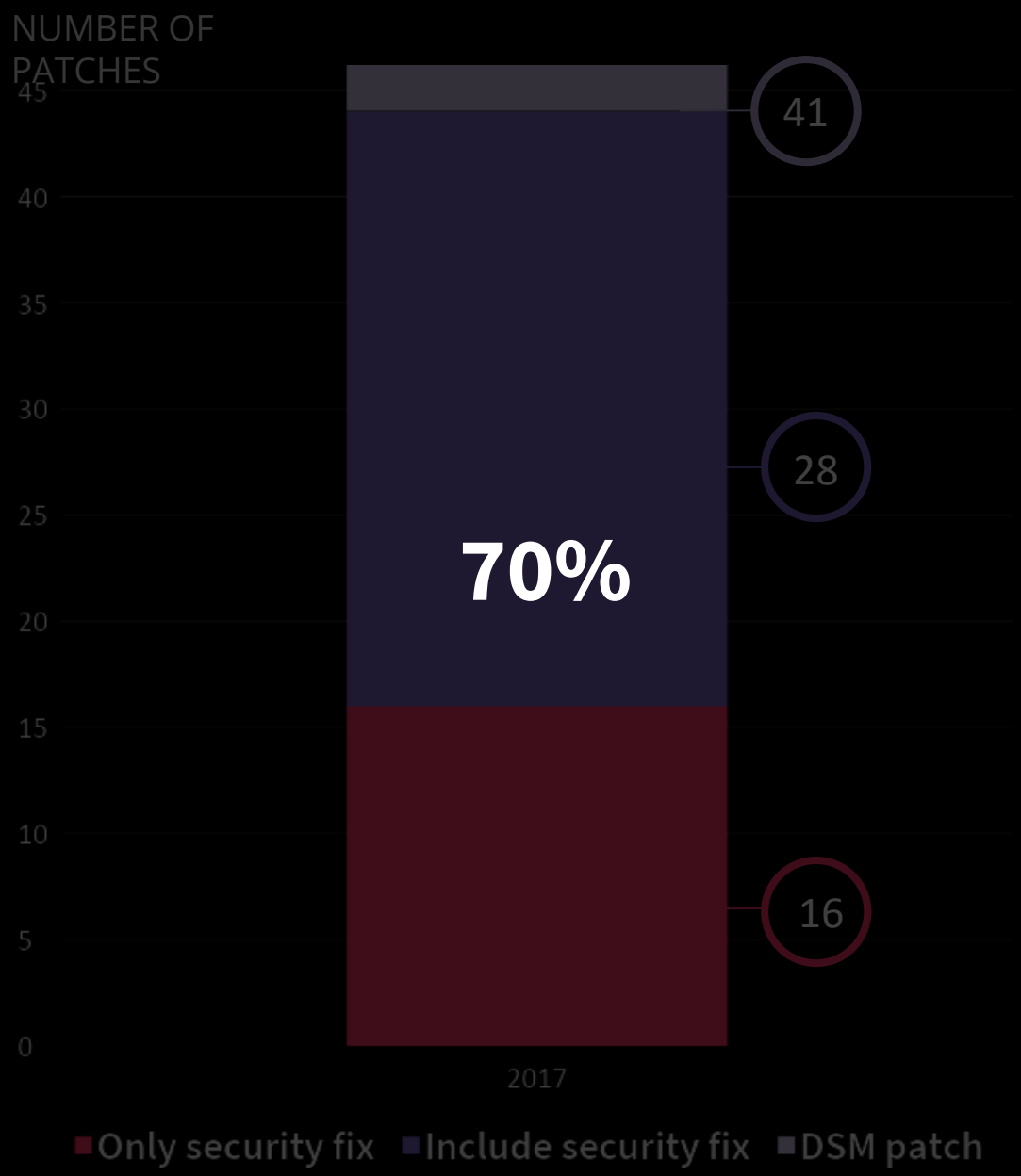
Incident response

# Software Release



Incident response

# Software Release



## Re: Security update CVE-2017-7494 for DSM 5.2 ??

by **gentilkiwi** » Sun Jun 04, 2017 12:54 am

Amazing to see the build was ready for 5.2 only 2 days after 6.1... good technical job (not on the communication part 🙂)




**DSM Update version 6.1.3-15152-1** (self.synology)

Sneeuwvlok 於 1 天前 發表

(2017-07-19)

Important Note

- The update is expected to be available for all regions within the region may vary slightly.

Fixed Issues

- Fixed a security vulnerability regarding Samba (CVE-2017-1110

Synology pushing out updates like crazy, +1 Synology!

**Simone Margaritelli** @evilsocket · May 10

Which vendor has better quality NAS devices? ( requirements: 2 bays, diskless, RAID 1, ssh+smb+nfs )

39% Synology

14% Western Digital

25% QNAP

22% Other

93 votes • Final results

6 4 3

**Bitquark**
@Bitquark

Follow

Replying to @evilsocket

Synology devices are nice, and they actually seem to care about security.

4:27 PM - 10 May 2017

# Synology PSIRT Framework

Synology

# Incident Response Flow

Synology

# Incident Response Flow

- Report
- Triage
- Remediation
- Disclosure

Synology

- Report

# Incident Response Flow

# Incident Response Flow

- Report
- Triage

Synology

# Incident Response Flow

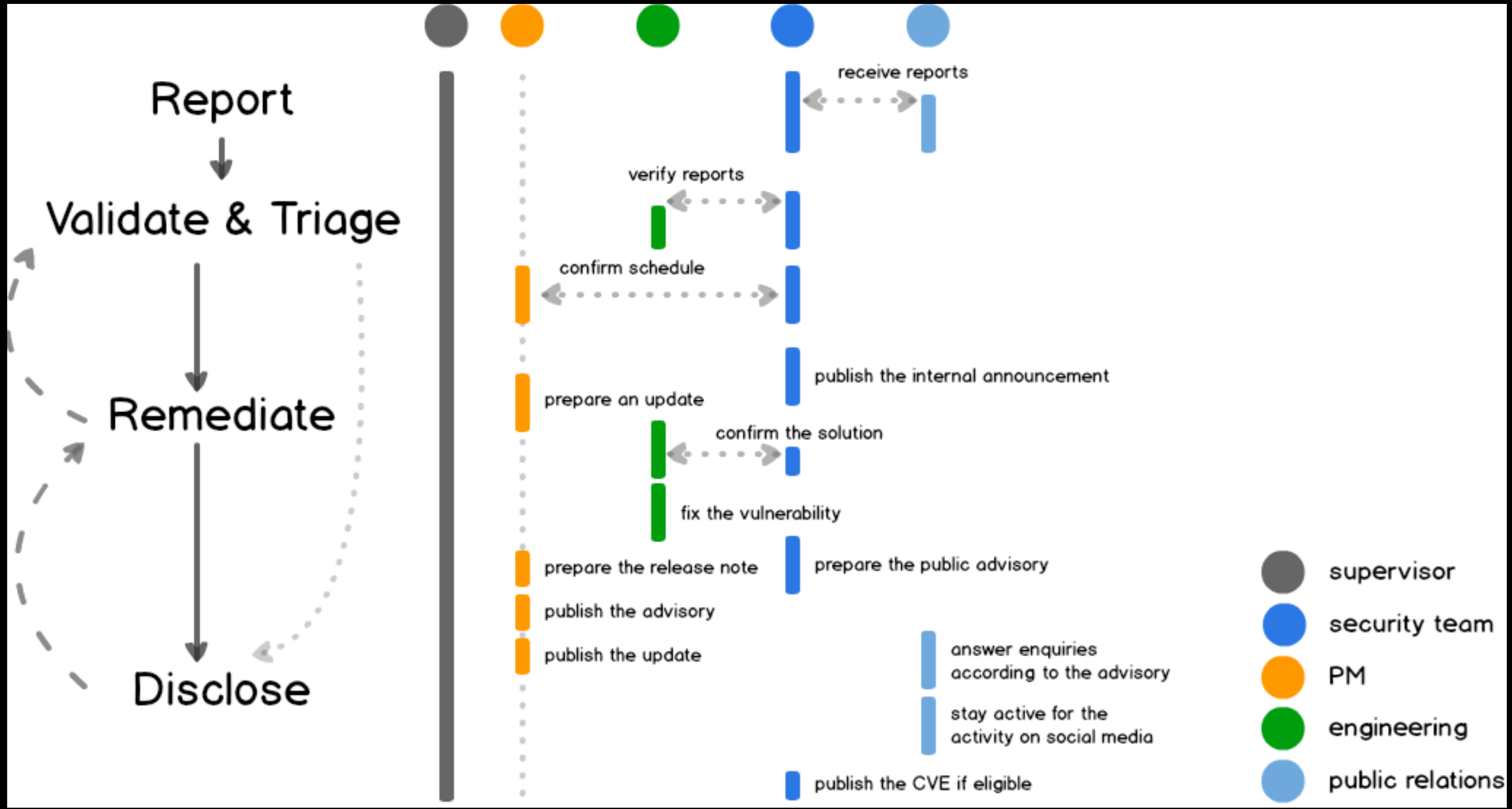
- Report
- Triage
- Remediation

Synology

# Incident Response Flow

- Report
- Triage
- Remediation
- Disclosure

Synology


Report
Validate & Triage
Remediate
Disclose
receive reports
verify reports
confirm schedule
publish the internal announcement
prepare an update
confirm the solution
fix the vulnerability
prepare the release note
prepare the public advisory
publish the advisory
publish the update
answer enquiries according to the advisory
stay active for the activity on social media
publish the CVE if eligible
supervisor
security team
PM
engineering
public relations

# Traffic Light Protocol

Synology

# Traffic Light Protocol Purpose

- Sensitive information control
- Color to separate level
- Easy applied to different channel

# Traffic Light Protocol Color

- TLP:RED
- TLP:AMBER
- TLP:GREEN
- TLP:WHITE

# TLP:RED

- Extreme Sensitive Information
- Impacts on a party's privacy, reputation, or operations
- May not share information with any parties outside of the specific exchange, meeting, or conversation.

Synology

# TLP:AMBER

- Requires support to be effectively acted upon
- Impacts on a party's privacy, reputation, or operations, if shared outside of the organizations involved.
- May share information with members of their own organization

Synology

# TLP:GREEN

- Awareness of all participating organizations
- Peers within the broader community or sector.
- May share information with peers and partner organizations, but not via publicly accessible channels.

Synology

# TLP:WHITE

- Minimal or no foreseeable risk of misuse
- Information may be distributed without restriction

Synology

# Product Life Cycle

Synology

# Synology Products

- Hardware: NAS, Router, Surveillance
- OS: DSM, SRM, VS960HD
- Packages: Multimedia, Collaboration
- Mobile and Desktop Application

Synology

DSM

# RELEASE LIFECYCLE MANAGEMENT

## General Availability

**FEATURES**
**FULL SECURITY**
**FIXES**

## Production Stage “2”

**HIGH/CRITICAL SECURITY**
**FIXES**

## Extended Life Stage

**BASED ON**
**EVALUATION**

## End of Life

Synology

DSM

# RELEASE LIFECYCLE MANAGEMENT

| | General Availability | End of Production | PHASE 1 | PHASE 2 | End of Life |
|---|---|---|---|---|---|
| **5.2** LTS | **5 / 2015** | **6 / 2016** | **6 / 2017** | **6 / 2019** | |
| **6.0** | **3 / 2016** | **6 / 2017** | **6 / 2018** | **-** | |
| **6.1** | **3 / 2017** | **6 / 2018** | **6 / 2019** | **-** | |
| **6.2** LTS | **5 / 2018** | **6 / 2019** | **6 / 2020** | **2022** | |

Synology

# Severity  Rating

Synology

# Synology Severity Rating

- Critical
- Important
- Moderate
- Low
- Not Affected

Synology

# Severity Rating
# Critical Impact

- Highly risky for systems that have not been fixed
- Needs to be fixed as soon as possible
- Possible to be automatically exploited by Unauthenticated remote attackers

Synology

# Severity Rating
# Important Impact

- No immediate impact on unfixed systems
- Should be fixed ASAP if services are provided to authenticated remote users
- Suggested to apply mitigations before the next system maintenance cycle

Synology

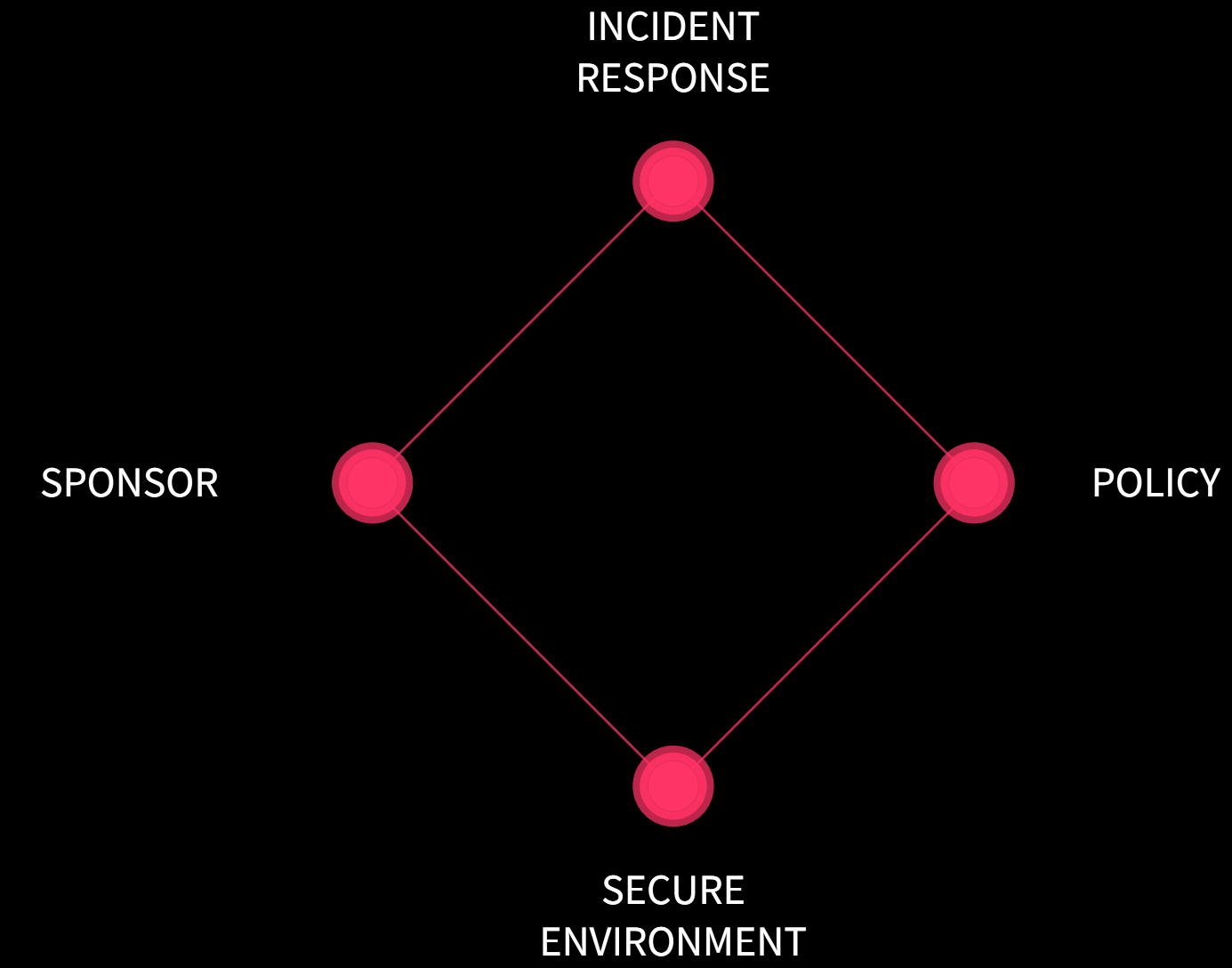
# Security Organization

Synology


FIRST
Improving Security Together
Panasonic
Microsoft
amazon
Synology
CISCO

Security organization

# FIRST




Synology

Security organization

FIRST

Panasonic

SPONSOR

TWCERT Coordination Center

Synology

# MITRE

Synology

# Further Commitment to Security

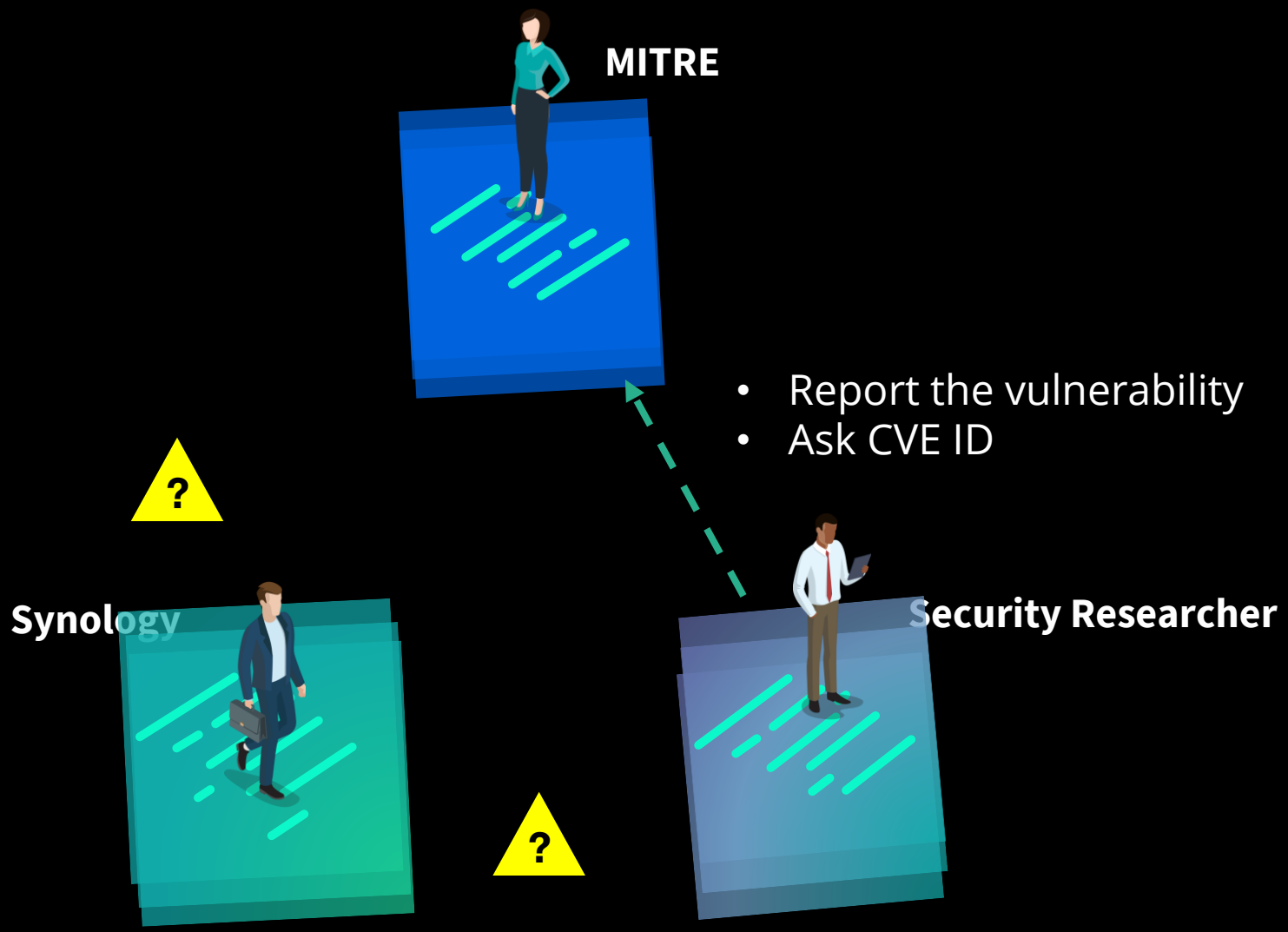
Synology is recognized as a CNA by The MITRE Corporation.
Detect threats better. Respond to vulnerabilities faster. Keep data safer.

Learn more

Synology

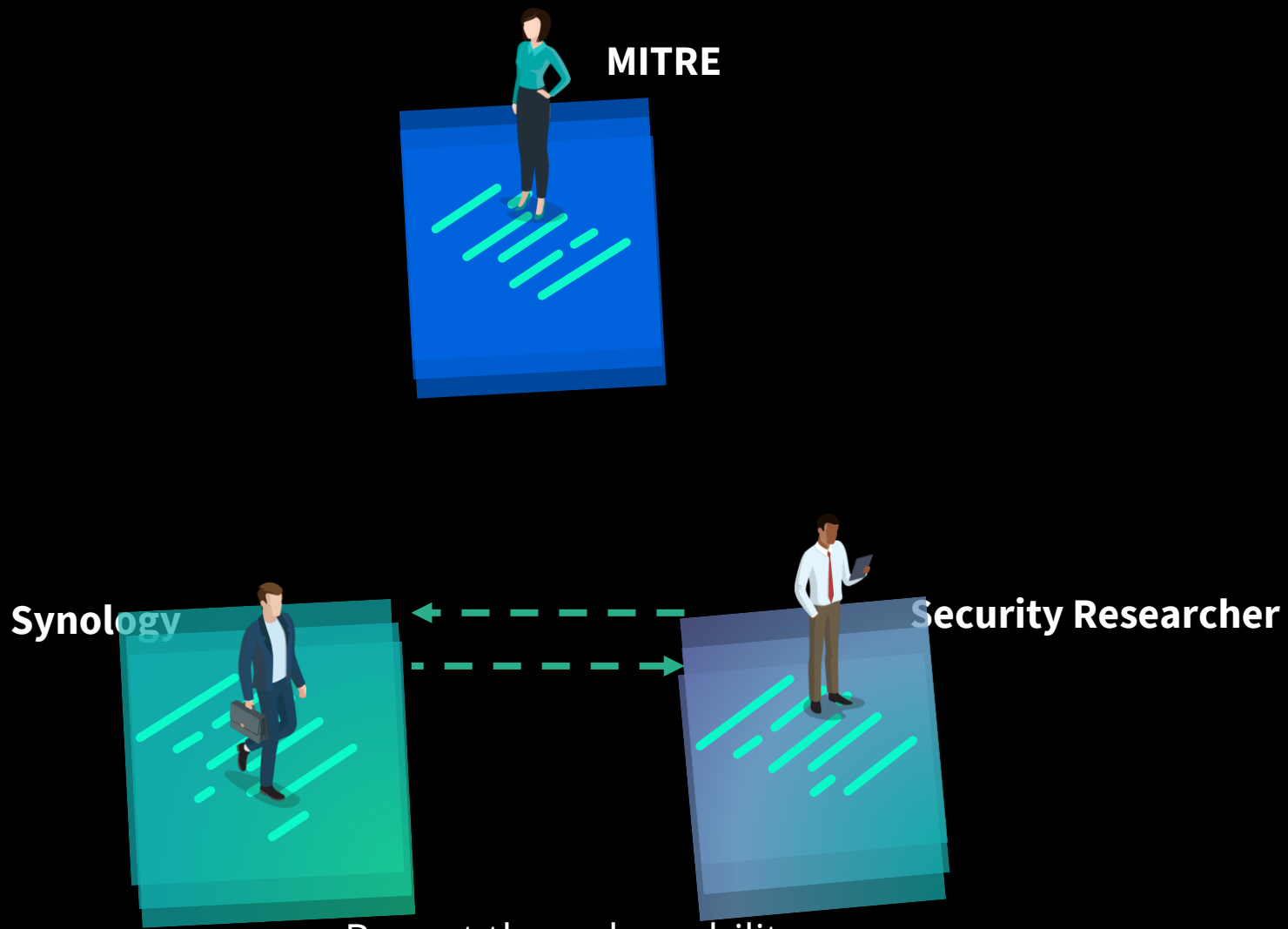
Security organization

# MITRE



Security organization

# MITRE




- Report the vulnerability
- Ask CVE ID
- Discuss the disclosure schedule

# Become CNA

- Schedule Control
- Transparent Communication with Researcher

Synology

# Synology Bounty Program

Synology

Hacker community

# BOUNTY PROGRAM

129

VALIDATED REPORTS
9/2017 – 6/2018

42,000 +

REWARDS (USD)
9/2017 – 6/2018

Synology

Hacker community

# BOUNTY PROGRAM

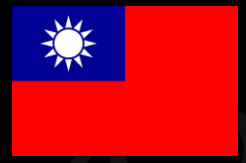
hackerone

Synology

# BOUNTY PROGRAM


Iran


India

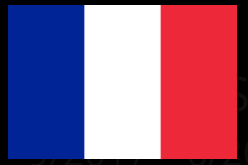

Taiwan


Pakistan


Hong Kong


Austria


Netherlands


France


Argentina


Spain

Synology

# BOUNTY PROGRAM


## Acknowledgement

We would like to thank the following researchers and parties for helping to improve Synology's product security:

If you would like to have your name listed on our acknowledgement page after the vulnerabilities you reported have been disclosed, please let us know when sending bug reports to us.

2018 2017

- Muhammad Junaid Abdullah (https://twitter.com/snoviboy)
- Kishan kumar (https://facebook.com/noobieboy007)
- Lays (http://l4ys.tw)
- Ashish Kumar (https://www.facebook.com/buggyashish)
- Lakshay Gupta (http://linkedin.com/in/lakshay-gupta-44102a143)
- Meng-Huan Yu (https://www.linkedin.com/in/cebrusfs/)
- Ifrah Iman (http://www.ifrahiman.com)
- Mohammed Israil (https://www.facebook.com/VillageLad, https://www.linkedin.com/in/mohammed-israil-221656128)
- Taien Wang (https://www.linkedin.com/in/taienwang/)
- Emad Shanab (@Alra3ees) (https://twitter.com/Alra3ees?s=09)
- குகன் ராஜா (Havoc Guhan) (https://fb.com/havocgwen)
- Yasser Gersy (https://twitter.com/yassergersy)
- Ismail Tasdelen (https://www.linkedin.com/in/ismailtasdelen)
- Thomas Fady (https://www.linkedin.com/in/thomas-fady)
- Oliver Kramer (https://www.linkedin.com/in/oliver-kramer-670206b5)

# Response Disclosure Policy

- 90-day responsible disclosure policy timeline
- 14-day grace period for high risk vulnerabilities
- corresponding security advisories are provided
- vulnerabilities details will not be disclosed


D-Day
D+1
D+90
D+104
grace period
report received
report acknowledged
report validated
vulnerability triaged
remediation
advisory published
reward remitted
CVE disclosed
advisory updated

# Conclusion

- Fast Incident Response Flow
- Security Organization
- Vulnerabilities Discovery

Synology

Thank you