SAN Case Study

National Cybersecurity Assessments and Technical Services (NCATS)

Presented By:
Jessica Bishop, Director of Information & Technology Services

SAN DIEGO INTERNATIONAL AIRPORT
LET'S GO.

NCATS Offerings

The NCATS team is a component of the DHS and supports Federal, State and Local governments and critical infrastructure partners by providing proactive testing and assessment services

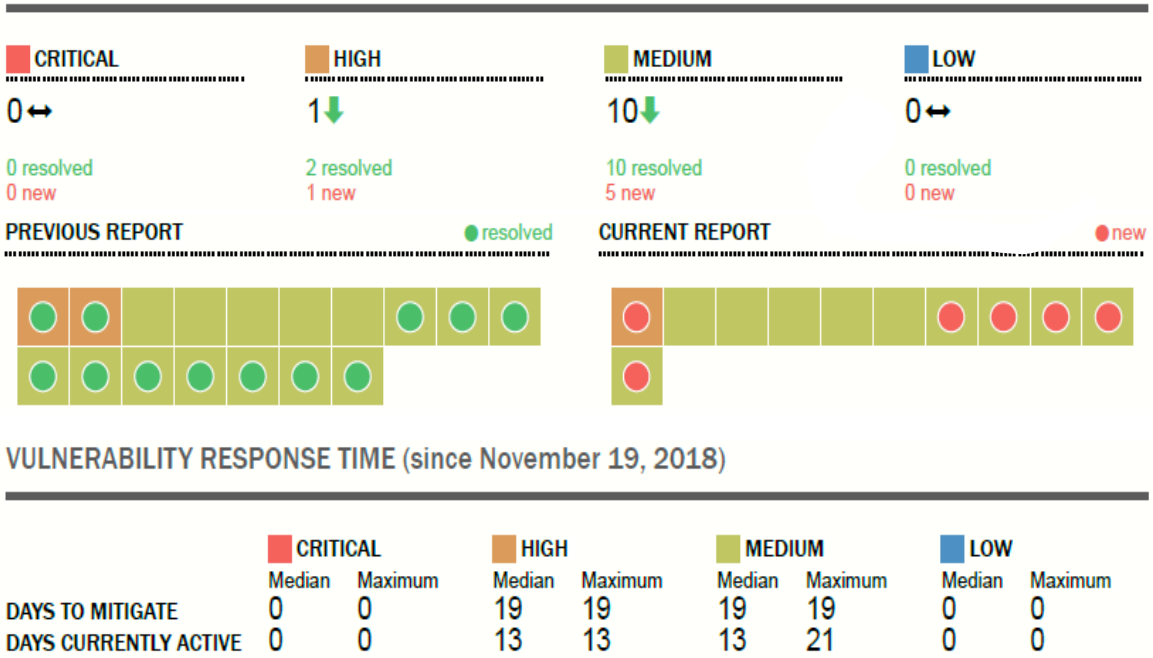
- **Cyber Hygiene Vulnerability Scanning**
- **Phishing Campaign Assessment (PCA)**
- **Risk and Vulnerability Assessment (RVA)**
- Validated Architecture Design Review (VADR)

All services are available at no cost!

Cyber Hygiene Vulnerability Scanning

Weekly scheduled vulnerability scans of Internet facing hosts

- Open insecure ports
- SSL validations
- Week encryption
- Insecure authentication configurations
- DNS weaknesses



VULNERABILITY REPORT CARD

Cyber Hygiene Vulnerability Scanning

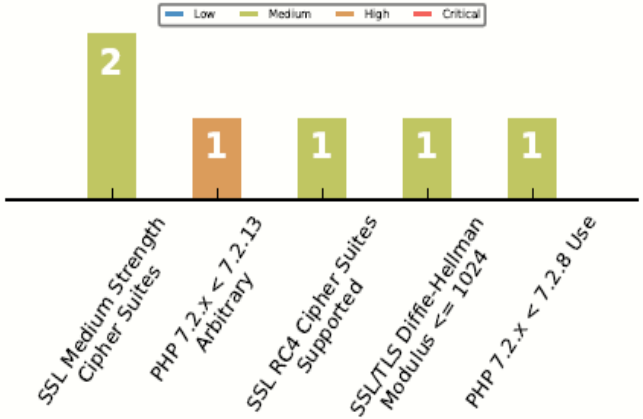


Figure 1: Top Vulnerabilities by Occurrence

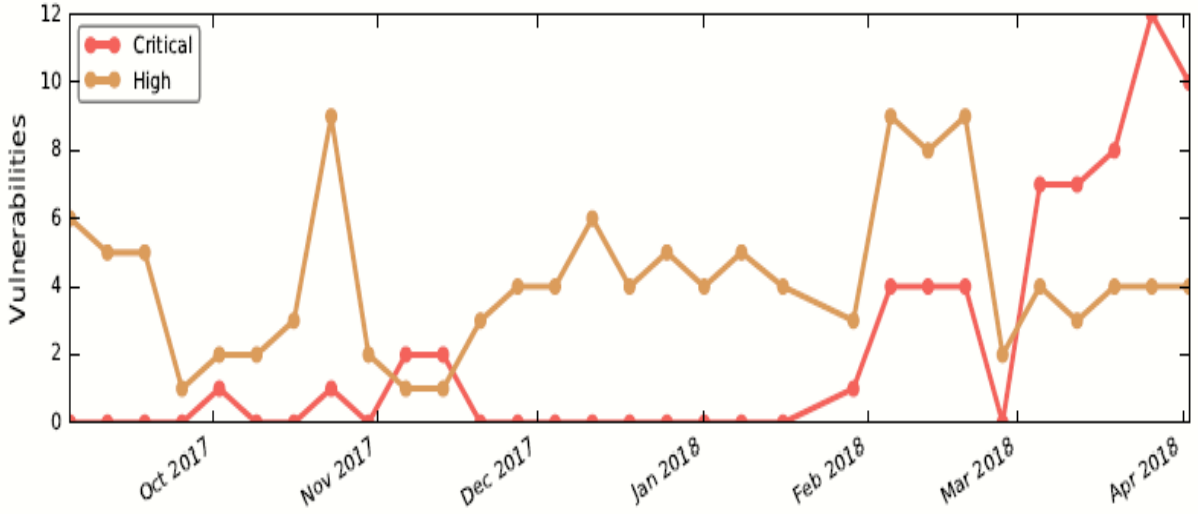
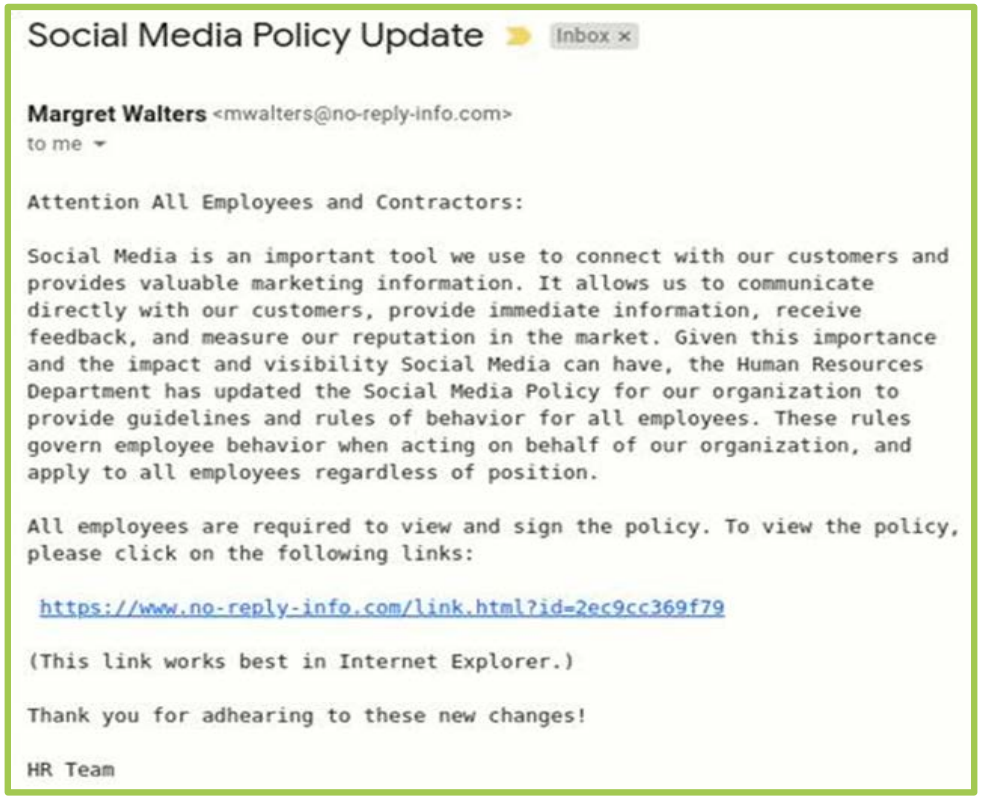


Figure 12: Active Critical and High Vulnerabilities Over Time

ASSESSMENT SUMMARY

Phishing Campaign Assessment (PCA)



Social Media Policy Update Inbox ×

Margret Walters <mwalters@no-reply-info.com>
to me

Attention All Employees and Contractors:

Social Media is an important tool we use to connect with our customers and provides valuable marketing information. It allows us to communicate directly with our customers, provide immediate information, receive feedback, and measure our reputation in the market. Given this importance and the impact and visibility Social Media can have, the Human Resources Department has updated the Social Media Policy for our organization to provide guidelines and rules of behavior for all employees. These rules govern employee behavior when acting on behalf of our organization, and apply to all employees regardless of position.

All employees are required to view and sign the policy. To view the policy, please click on the following links:

https://www.no-reply-info.com/link.html?id=2ec9cc369f79

(This link works best in Internet Explorer.)

Thank you for adhearing to these new changes!

HR Team

Determine the susceptibility of staff and infrastructure to phishing attacks

- Phishing click rate 5%
- Imbedded beacon on workstation
- Harvested SPN ticket hashes
- Decrypted password hashes
- Enumerated accounts for elevated access

…..so what did we learn?

Risk and Vulnerability Assessment (RVA)

Determine what impact an internal attacker or disgruntled employee could have with access to the internal network

- Provided access to our network
- Located a device with default manufacturer credentials
- Configured the device to send traffic to their laptop
- Captured encrypted credentials

…..so what did we learn?

NCATS Enrollment

ncats_info@hq.dhs.gov