viettel security

PENTESTING IN DEPTH

Hà Nội – 05/2023

1

viettel security

NỘI DUNG

- DỊCH VỤ PENTESTING
- PENTESTING IN DEPTH
- DỊCH VỤ DEVSECOPS
- TỔNG KẾT

2

viettel security

TOP ATTACK VECTOR

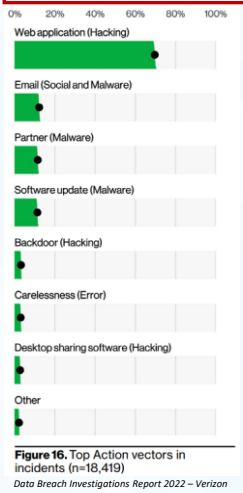


Figure 16. Top Action vectors in incidents (n=18,419)

Data Breach Investigations Report 2022 – Verizon

3

3

viettel security

PENTEST

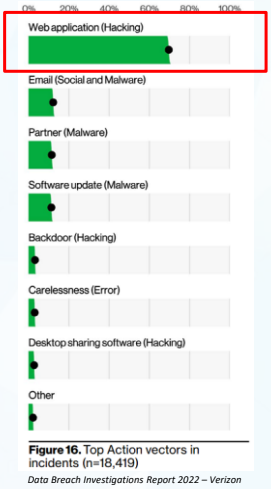


Figure 16. Top Action vectors in incidents (n=18,419)

Data Breach Investigations Report 2022 – Verizon

Dịch vụ đánh giá ATTT ứng dụng (Pentest)

Mục đích:
- Tìm hết các lỗ hổng security của ứng dụng.
- Đi trước attacker.

Đối tượng:
- Website
- App mobile
- App desktop

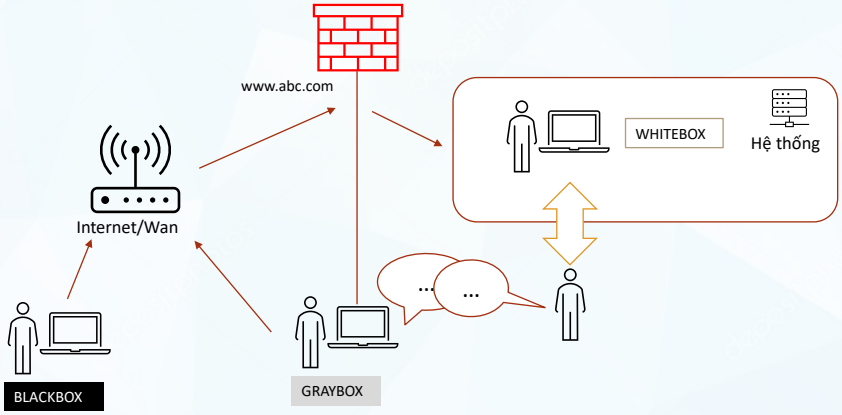
WHITEHAT

4

4

viettel security

CÁC HÌNH THỨC PENTEST

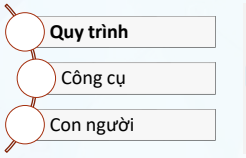


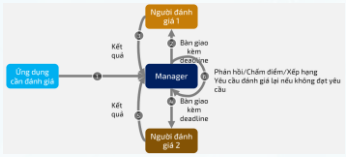
5

5

viettel security

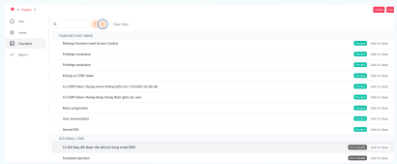
VCS PENTEST





- Quy trình **check chéo** Multiple-check.
- Chuẩn hóa **checklist** các công việc cần thực hiện
- Chuẩn hóa **danh mục lỗ hổng**.
- Chuẩn hóa **Workload**.

VCI	Category
VCI-01	Application-Level Denial-of-Service (DoS)
VCI-02	Broken Access Control (BAC)
VCI-03	Broken Authentication and Session Management
VCI-04	Broken Cryptography
VCI-05	Client-Side Injection
VCI-06	Cross-Site Request Forgery (CSRF)
VCI-07	Cross-Site Scripting (XSS)
VCI-08	External Behavior
VCI-09	Insecure Data Storage
VCI-10	Insecure Data Transport
VCI-11	Insecure OS/Firmware
VCI-12	Insufficient Security Configurability
VCI-13	Lack of Binary Hardening
VCI-14	Logical Issues
VCI-15	Mobile Security Misconfiguration
VCI-16	Network Security Misconfiguration
VCI-17	Privacy Concerns
VCI-18	Sensitive Data Exposure
VCI-19	Server Security Misconfiguration
VCI-20	Server-Side Injection
VCI-21	Unvalidated Redirects and Forwards
VCI-22	Using Components with Known Vulnerabilities



OWASP

bugcrowd

6

6

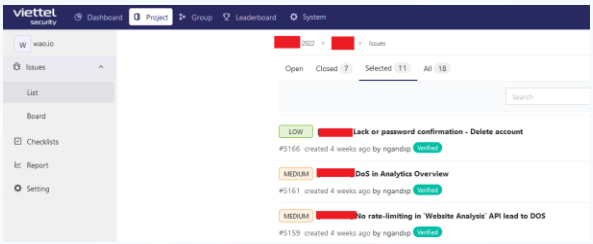
viettel security

VCS PENTEST

- Quy trình
- **Công cụ**
- Con người

xPentest Platform

- **Kiểm soát** chất lượng report đầu ra, năng suất lao động, chất lượng thực hiện của pentester.
- Quản lý, tương tác, **tối ưu kết quả** pentest, checklist.
- **Flexiable** trong triển khai dịch vụ.
- Quản lý **vòng đời lỗ hổng**.



7

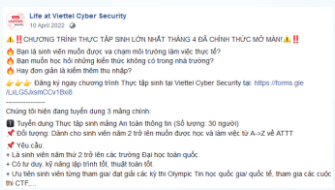
7

viettel security

VCS PENTEST

- Quy trình
- Công cụ
- **Con người**

- Nhân sự chất lượng cao từ nguồn **VCSLab**.
- 100% nhân sự được **chuẩn hóa** thông qua:
  - Chứng chỉ: OSCP, OSWE, PortSwigger.
  - Kết quả nghiên cứu: CVE, Bugbounty
- **Hợp tác** cùng các trường đại học, trung tâm đào tạo để được tiếp nhận nhân sự đầu ra chất lượng cao.
- Liên tục **Đào tạo** các lứa nhân sự kế cận bằng các chương trình đào tạo được thiết kế chuyên biệt.

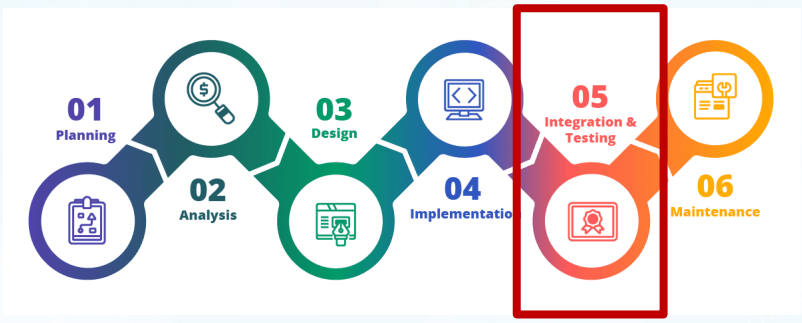


8

8

viettel security

PENTEST KHI NÀO?



Chốt chặn trước khi release trong **quy trình phát triển phần mềm**

9

9

viettel security

AN TOÀN TUYỆT ĐỐI CHƯA?

Không có khái niệm an toàn tuyệt đối trong một hệ thống CNTT.

Có nhiều nguyên nhân:
- Vận hành
- 0day
- Các bản cập nhật
- Các thành phần khác liên quan

10

10

viettel security

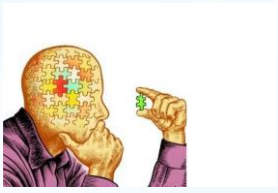
PENTESTING IN DEPTH

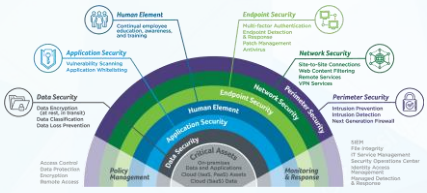
11

viettel security

DEFENSE IN DEPTH

- Không có khái niệm an toàn tuyệt đối trong Security.
  - Tăng phản biện.
  - Tăng góc nhìn.





12

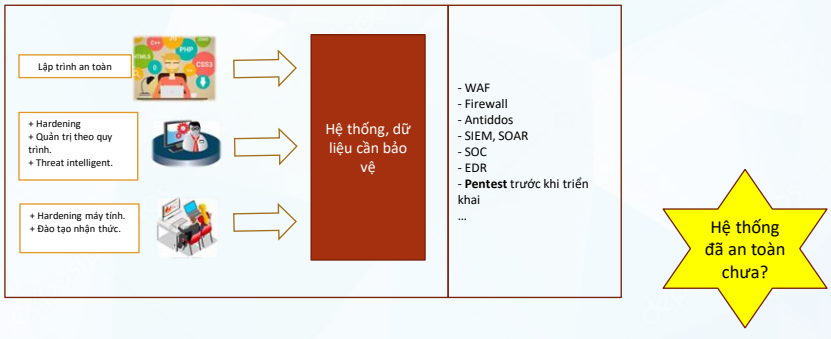
12

TĂNG PHẢN BIỆN

13

viettel security

CÂU HỎI VỀ MỨC ĐỘ HIỆU QUẢ



14

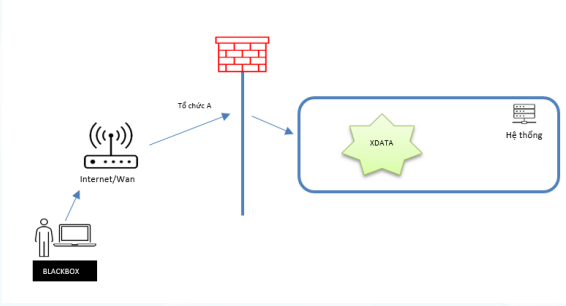
14

viettel security

REDTEAM

Tập trung vào mục tiêu trọng yếu mà khách hàng quan tâm mức độ an toàn. Nhóm triển khai sẽ tập trung khai thác để tìm cách xâm nhập, tiếp cận vào mục tiêu.

- ✓ Đánh giá lại hiệu quả đầu tư ATTT.
- ✓ Rèn luyện thực chiến cho bộ phận ATTT nội bộ.



15

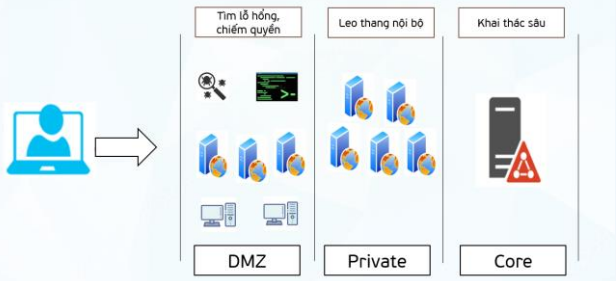
15

viettel security

REDTEAM

Mô phỏng sát nhất với các cuộc tấn công APT, dịch vụ Redteam sẽ được triển khai tấn công toàn diện theo chuỗi Kill-Chain và trên cả 3 hướng:

- Hệ thống **public Internet**: các hệ thống public Internet sẽ được xem xét và tìm cách xâm nhập, khai thác để đi sâu vào trong.
- **Người dùng**: bằng các nghiệp vụ phishing, scam, khai thác email, … đội tấn công sẽ tìm cách xâm nhập vào máy tính người dùng, từ đó khai thác sâu vào các hệ thống nội bộ.
- Đường **vật lý, social engineering**: trong trường hợp cần thiết, đội tấn công sẽ tiếp cận trực tiếp các cửa hàng, chi nhánh để rà quét wifi, các đường mạng, các đường USB để tìm đường leo thang.



16

16

viettel security

RỦI RO ẢNH HƯỞNG HỆ THỐNG

1. Dịch vụ cam kết SLA không làm ảnh hưởng đến hoạt động hệ thống
2. Các hành động tác động vào hệ thống đều được lưu lại vết và nằm trong danh sách hành động được phép.
3. Tác động được đánh giá theo khung CIA:

- Các hành động ảnh hưởng tính **availability**: Không thực hiện
- Các hành động ảnh hưởng tính **integrity**: Chỉ thực hiện triển khai tool lên các host chiếm quyền được, tool này ở dạng mức file, không cài đặt backdoor sâu. Không thực hiện thay đổi đối với dữ liệu của tổ chức.
- Các hành động ảnh hưởng tính **confidently**: Chỉ dùng thông tin credential thu thập được để leo thang vào các máy chủ mục tiêu (các credential này được cung cấp lại và có thể đổi ngay sau diễn tập). Không collect database của tổ chức.

17

17

TĂNG GÓC NHÌN

18

viettel security

VẪN BỊ HACK

16-Year-Old Teen Hacked Apple Servers, Stole 90GB of Secure Files

Aug 17, 2018

Well, there's something quite embarrassing
Though Apple servers are widely believed t

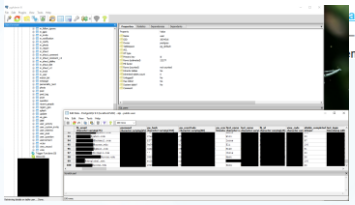
4. LinkedIn

Date: June 2021
Impact: 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting

1. Yahoo

Date: August 2013
Impact: 3 billion accounts



Adobe Breach Impacted At Least 38 Million Users

October 29, 2013 — 73 Comments

The recent data breach at **Adobe** that exposed user account information and prompted a flurry of password reset emails impacted at least 38 million users, the company now says. It also appears that the already massive source code leak at Adobe is broadening to include the company's **Photoshop** family of graphical design products.

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

19

19

viettel security

BUG BOUNTY

- Bắt đầu xuất hiện từ 1995 (Netscape)
- Nở rộ từ 2014 với sự thành lập của HackerOne, BugCrowd
- Tạo ra sự kết nối giữa hacker và doanh nghiệp

Khanh Ta
@anotherkhanhtq

Just received the notification from @immunefi. Huge thanks to very supportive @OxMackenzieM

Dịch Tweet

Thanks for your patience. Severity: Critical Case: #17823 Amount: $250,000
Rate: [redacted]

10:53 · 26 thg 4 23 · **62,5K** Lượt xem

Kỹ sư Việt kiếm trăm nghìn USD từ lỗ hổng Microsoft, Oracle

Nhóm năm kỹ sư trẻ Việt Nam, sinh từ năm 1999 đến 2003, giành 115.000 USD vì khai thác thành công lỗ hổng của Microsoft Teams và Oracle VirtualBox.

Theo bảng xếp hạng cuộc thi Pwn2Own Vancouver vừa được công bố, đội thi của nhóm kỹ sư Việt Nam xếp hạng ba với 12 điểm, đứng sau hai đội Synacktiv của Pháp và STAR Labs từ Singapore.

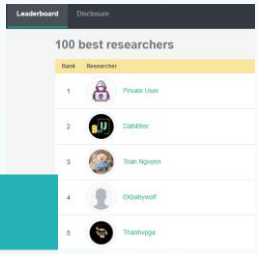
20

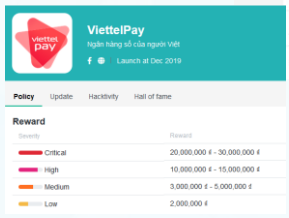
20

viettel security

DỊCH VỤ SAFEVULN

- Nền tảng hoạt động theo cơ chế **Bugbounty**.
- Hơn 100 **reseachers** thường xuyên hoạt động.
- Có thể áp dụng thành kênh quản lý **vulnerabilites disclosure**.





21

21

DEVSECOPS

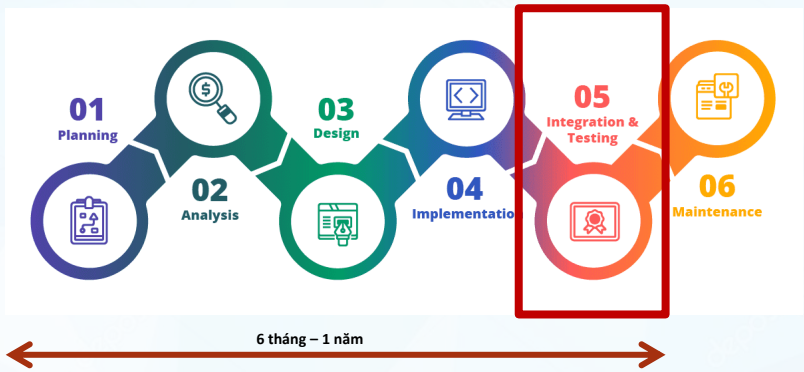
Bức tranh trước pentest

22

22

viettel security

WATERFALL

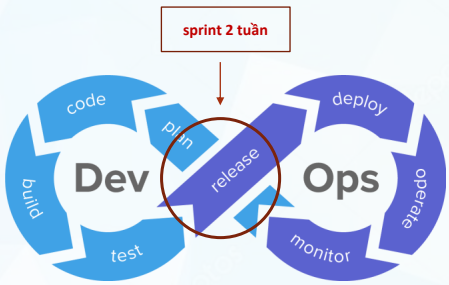


23

23

viettel security

DEVOPS



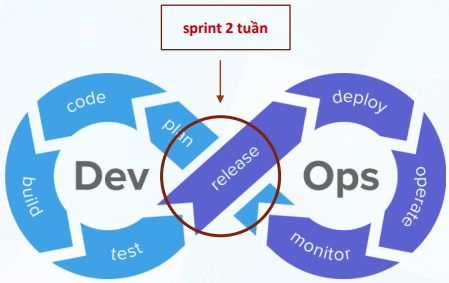
- Thu hẹp khoảng cách Developer và Operator
- Rút ngắn thời gian release
- Thích ứng nhanh

24

24

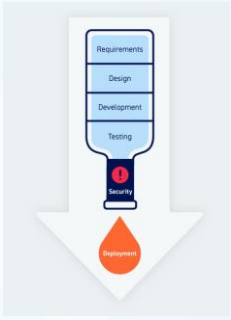
viettel security

DEVOPS



- Thu hẹp khoảng cách Developer và Operator
- Rút ngắn thời gian release
- Thích ứng nhanh

- Dịch vụ pentest khó theo kịp được tiến độ.
- Văn hóa DevOps là không phụ thuộc vào Gate

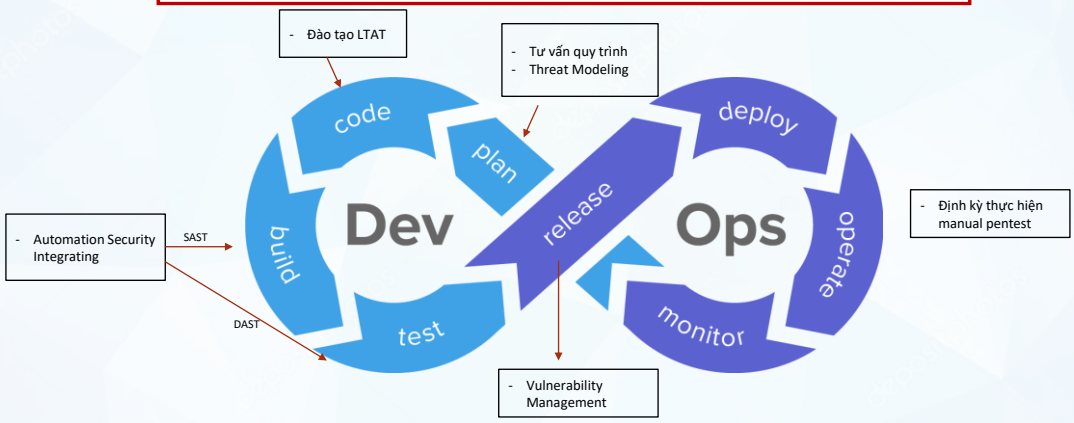


25

25

viettel security

VCS DEVSECOPS

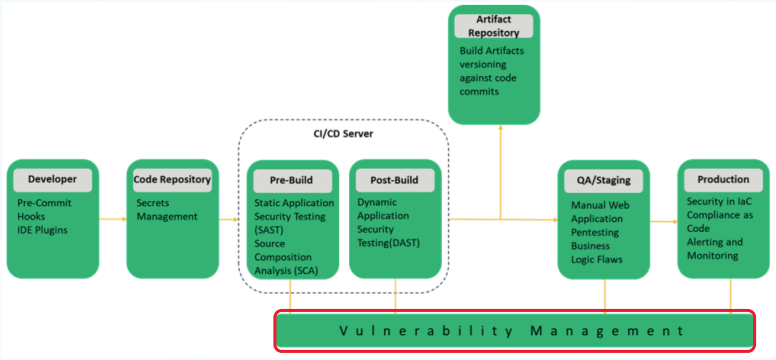


26

26

viettel security

AUTOMATION SECURITY INTEGRATING

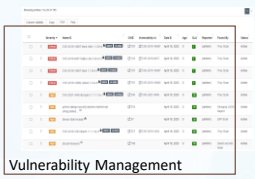


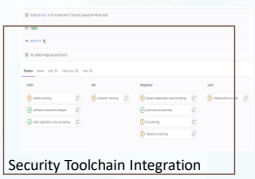
27

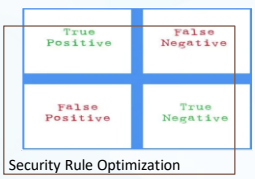
27

viettel security

AUTOMATION SECURITY INTEGRATING


Vulnerability Management


Security Toolchain Integration



Security Rule Optimization

28

28

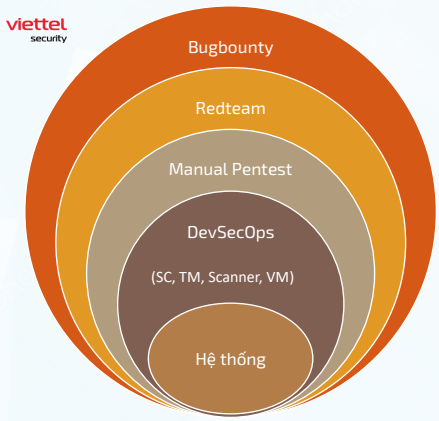
TỔNG KẾT

29

29

viettel security

PENTESTING IN DEPTH



30

30

THANK YOU

cuongmx@viettel.com.vn

31