Offensive Security Testing

lundi de la Cybersécurité

13 mai 2024

Agenda

1. Who’s speaking ?
2. Context
3. CyberSec as usual
4. Offensive Security Testing
5. DevSecOps 4 real
6. Successful Bug Bounty
7. Conclusion
8. Q&A

00

Who’s speaking ?

Nicolas Kalmanovitz
COO @ Yogosha
n.kalmanovitz@yogosha.com
@kalmanovitzN

Who's speaking ?

Not an expert but **an enlightened fan !**

- 25 years of software development
- COO & CPO @Yogosha
- Risk Owner
- ex Octo Technology - Accenture
- ex meetic - match.com

❤ CISO, CSIRT, SOC, Blue Team, ...

❤ Security Researchers, Pentesters, Ethical Hackers, Red Teams, ...

❤ Program Security Managers, Security Analysts, Triagers, ...

01

Context

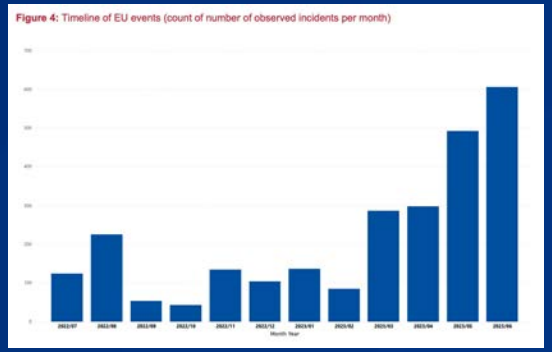
The good old days

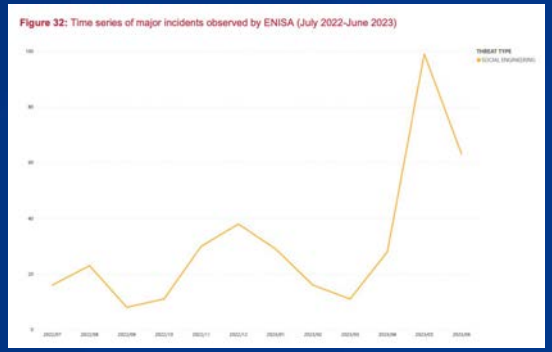
- Low number of assets to be audited
- Occasional releases, stable applications
- Limited intrusion techniques
- Enough available Cybersecurity professionals

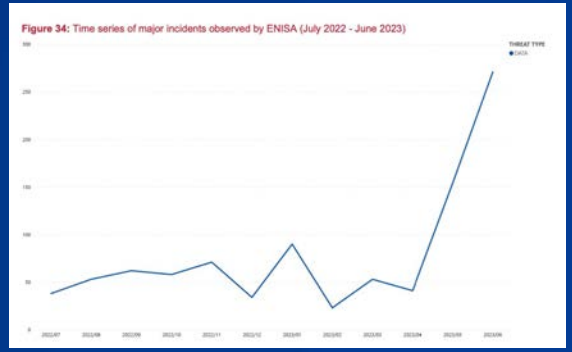
The present struggles

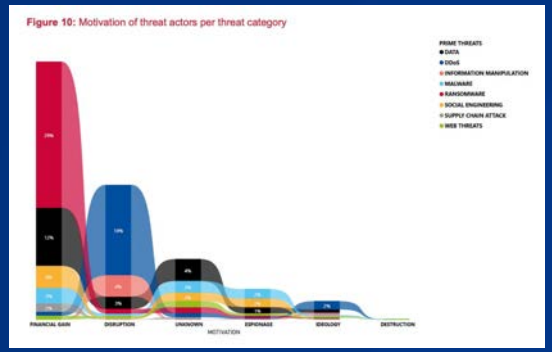
- The number of assets to audit is increasing exponentially
- There are numerous developments requiring frequent updates
- Technological transformations (AI, Crypto, IoT, etc.) are both very rapid and unpredictable
- Intrusion techniques are numerous
- Cybersecurity is experiencing a severe skills shortage

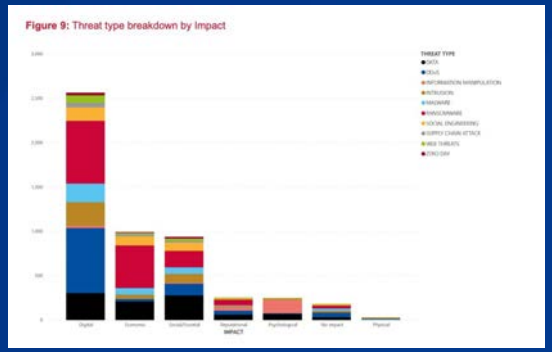
Intensification of cyber attacks

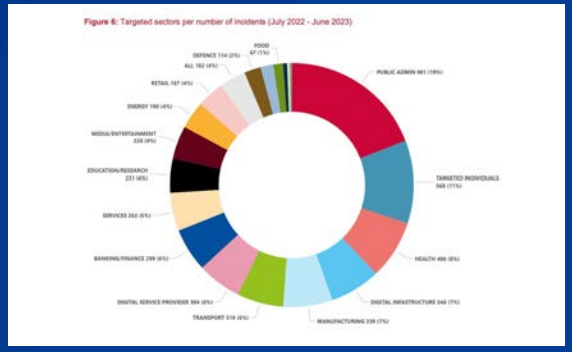












yogosha
Vulnerability Operation Center

- **73% of internet traffic** to websites and apps between January and September 2023 was **malicious**
- **85% of organizations** suffered at least one successful **cyber-attack** last year

Arkose Labs 2023 reports

02

CyberSec as usual

Traditional approaches

Automated Scanners

- Fast, Scalable and Continuous
- Automated result, no validation
- High level of false/positives with poor signal-to-noise ratio
- No remediation support
- **Not able to find complex exploits**

Traditional Pentesting

- 1-3 persons for 1-2 weeks, once a year
- 4-6 weeks lead time
- Low cost rather than high quality
- Traditionally Compliance focused
- Does sophisticated Attack behavior
- **Many serious Vulnerabilities remain undetected**

03

Offensive Security Testing

yogosha
Vulnerability Operation Center

*A **proactive** cyber-security approach that involves actively testing a system's defenses by **simulating an adversary's actions.***

*The goal is to identify and **remediate** security vulnerabilities **before** a real attacker can **exploit** them. This practice may include **Penetration Testing as a Service, Bug Bounty**, VDP, Red Teaming, ...*

PenTest as a Service

PTaaS is an outsourced approach where penetration testing is managed via an **online platform** that allows users to schedule and conduct security tests **at their convenience** (on demand or continuous)**.** This method provides penetration testing , **real time** vulnerability management, detailed risk assessments, **direct interactions** with the pentesters and **remediation** recommendations.

Black Box
Realistically simulate an external attack with researchers who have no prior knowledge of an Information System

Grey Box
With some high-level information at their disposal, researchers can identify vulnerabilities within the reach of the most determined external attackers

White Box
By providing detailed information to researchers (infrastructure, source code, architecture, etc.), they can thoroughly evaluate the security level of most complex assets

- Flexibility and Frequency
- Compliance Objectives
- Cost efficiency
- Risk-Based Prioritization
- Results Mobilization
- Real time collaboration
- Integration with DevSecOps workflows

yogosha
Vulnerability Operation Center

*By 2026, organizations leveraging PTaaS will perform up to **10 times** more frequent pentesting and enable **2 times faster remediation** (...)*

Gartner *Innovation Insight: Penetration Testing as a Service* nov. 2023

Bug Bounty

Bug bounty is a method of detecting vulnerabilities, which involves using the **community of ethical hackers** to test the security of digital assets. It is a bug hunt that is based on a **pay-for-results** logic. Organizations offer monetary rewards—bounties—to hackers for each valid vulnerability they manage to identify. The more critical the vulnerability, the higher the reward. If no vulnerabilities are detected, the organization incurs no expense

Public Bug Bounty
It's a program open to all security researchers who wish to participate. The underlying assumption is that by increasing the number of participants, the chances of finding vulnerabilities are also increased.

Private Bug Bounty
It's a program open only to **invited researchers**. They are selected based on their specific skills, prior experience, or reputation. Private programs allow for closer **control** over who is testing the assets and provide a more secure environment for testing potentially **sensitive systems**.
#Black Box, #Grey Box

- Flexibility and Continuity
- Diversity of skills and approaches
- In-depth detection of critical vulnerabilities
- Cost efficiency
- Risk-Based Prioritization
- Results Mobilization
- Real time collaboration
- Retesting
- Continuous Integration with DevSecOps

yogosha
Vulnerability Operation Center

*In 2022, The number of software vulnerabilities found rose by 21%, with over **65,000 discoveries**;*

*Meta paid over **$2 million** in bounties and received 10,000 reports;*

***Critical vulnerabilities** were the top-paying, with **$61 million**, accounting for 92.7% of all bounties.*

GoGetSecure.com BugBounty Statistics

Continuous OffSec Testing

Continuous OffSec is an **emerging** approach where security testing is conducted **continuously** to identify and remediate vulnerabilities before they are exploited. It involves fully integrating Attack Surface Management tools and **collaborative and offensive** practices such as PTaaS and Bug Bounty into the **devsecops** workflow.

04

OffSec Testing Platform

Yogosha

Continuous OffSec

VPN & Monitoring

Asset Discovery
Detect changes in your Attack Surface

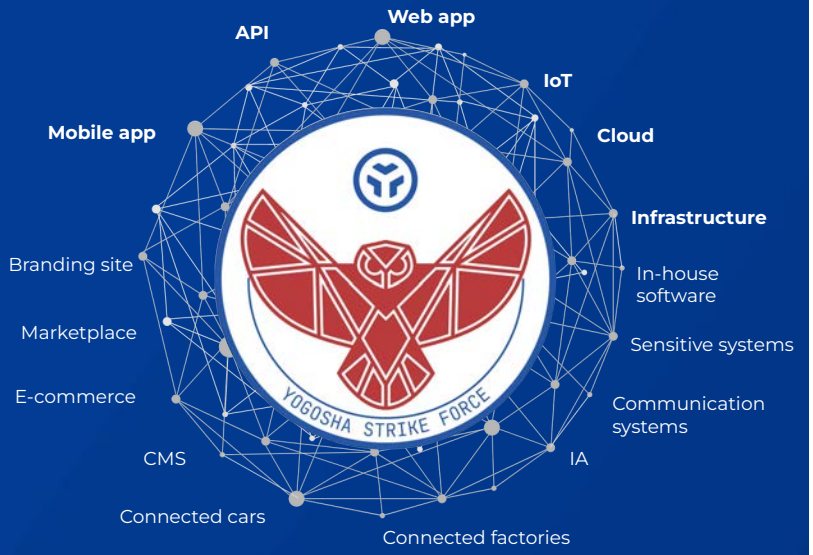
OffSec Testing Platform
PtaaS, Compliance, Bug Bounty, VDPs, Red Teaming, Code audit, ...

Security Researchers
>1000 researchers, skilled and background-checked

SaaS | Self-Hosted | On-premises

We bring together the best experts and tools to master vulnerabilities and protect society.

Vulnerability Reports → Triage → Remediation → Retest → Resolved → Analytics



Yogosha Strike Force

Specialized in finding critical vulnerabilities by simulating sophisticated and novel attacks produced by hackers

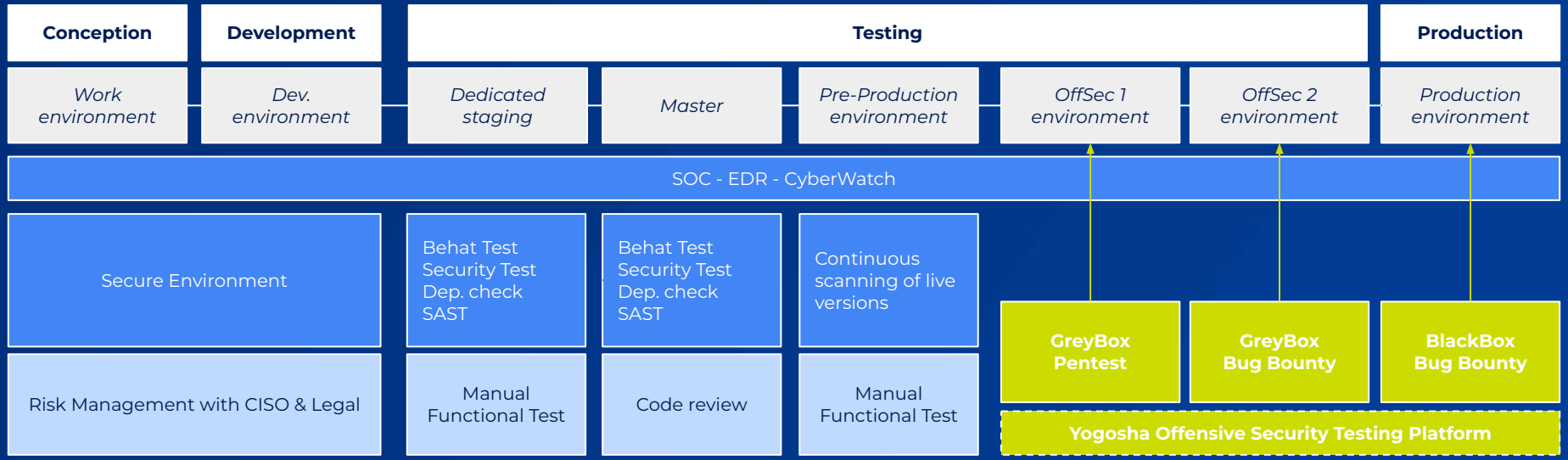
- Hundreds applications/month
- Acceptance rate : **10%**
- Technical tests
- Redactional tests
- ID & **Background check**
- Sign T&Cs with NDA
- Experienced in OWASP, ISSAF, OSSTMM, PTES, NIST
- Certifications (OSCP, OSEP, OSWE, OSEE, GXPN, GCPN, eWPTXv2, PNPT, CISSP)

05

DevSecOps 4real

DevSecOps @yogosha

A close and ongoing collaboration between CISO, Product, Dev, DevOps, Cyber Team & Security Researchers



Value Chain | *Environment* | Automation | Manual | **Offensive**

#ISO 27001

05

Bug Bounty Recipe

Are you ready ?

Bug bounty is not for immature assets.

Have you ever conducted a pentest?

If not, start there!

3 ingredients

- Program attractiveness
- Program management
- Remediation approach

Attractiveness

- Interesting Scope
- Clear Communication
- Effective Triage
- Timely payments
- Competitive Rewards
- Consistent Visibility

Prog. Mngt

- Notify the teams
- Educate the business units
- Organize triage
- Update program

Remediation

- A clear process
- Dedicated time
- Continuous improvement

08

Conclusion

Conclusion

- The threat is growing
- Traditional approaches are insufficient
- Ethical hackers are essentials
- Continuous Offensive Security testing is a key
- Integrate PTaaS and Bug Bounty into your DevSecOps
- Cybersecurity is at the heart of the value proposition
- and a societal commitment !

Hack4Values

CYBERSECURITY CHANGE MAKERS

The world-wide ethical hackers community

to protect the NGOs

10

Q&A


yogosha
Vulnerability Operations Center