COVID-19:
Changing the way we work in InfoSec

July 16th 2020
Speakers:

Rajendra Umadas
InfoSec Architect
Beyond Identity

Ivan Novikov
CEO
Wallarm

Yury Larichev
CRO
Wallarm

wallarm

Pandemic for InfoSec teams

What InfoSec managers say....

- Fast new solutions deployment (lack of resources, time constraints)
- Risks & processes control – all remote & at the last moment
- 9 out of 23.... Dealing with uncertainty: how long current situation will continue?

wallarm

Pandemic for InfoSec teams

From attackers' side....

- 2.2X attacks growth targeting API's and applications
- Large attacks volume impacts quality of events management & reaction time
- Increased workloads on applications makes attackers life easier (undetectable)

wallarm

IT challenged in WFH world

1. Remote access to corporate resources & services
2. Access rights & roles management
3. New tools implementation
4. Increased workload on current systems/tools
5. Increased attacks volume
6. Frozen IT budgets
7. Remote Support Desk

Please vote

wallarm

1. Remote access

- VPN
  - We have it for a while, why we keep having technical issues?
  - Settings & user's education
  - Mobile devices protection (BYOD)
- Control of mobile devices
  - BYOD (Bring Your Own Device)
  - COPE (Corporate Owned, Personally Enabled)
  - CYOD (Choose Your Own Device)

wallarm

2. Access rights management

- Undefined roles
- Undefined remote work processes
- Faster changes needed!
- No access control systems
- Risk management

wallarm

3. New tools deployment/intro

- Implementation process is broken due to sudden priority changes
- New policies implementation
- InfoSecurity systems implementation

wallarm

4. Increased workload on existing systems

- InfoSec systems are not ready
- False Positives became critical
- Systems inventory: suddenly, there are some which are not in use
- New use case scenarios (not covered by existing policy)

wallarm

5. Attacks volume increase

Attacks increase stats – Feb-May 2020 (YoY %)

- +20% for financial systems
- +90% for corporate sector & manufacturing
- + 130% for e-commerce

wallarm

6. Frozen IT budgets

- Damaged revenue flow puts IT budgets on hold (delayed projects)
- Approval (procurement) takes longer
- IT team cuts (layoffs)
- Increased workload on existing team (shared resources)
- Limited resources for any new toll deployment
- Complicated WFH logistics (fully remote IT infra management)

wallarm

Silver Linings and Surprises

1. Catalyst for pushing large change
    - Remote access to corporate resources & services
    - Access rights & roles management
2. Drive for efficiency
    - Frozen IT budgets
    - Increased workload on current systems/tools
3. Support distributed and asynchronous creative workflows
    - New tools implementation
4. Increased attacks volume
    - More data to feed back into your AppSec program

wallarm

Silver Linings and Surprises
#1 Large Change

Catalyst for pushing large change

- Remote access to corporate resources & services
  - Drive for SSO adoption with SAML and SCIM or other user provisioning flows
    - Easier for the user to get access day 1
    - Easier for the admin to provision, audit, and deprovision access
- Access rights & roles management
  - Pay back tech debt on implementations of policies and groups
    - Weedout the “one off task” done by IT staff during onboarding that gets fixed due to in-person onboarding
    - Fix or implement more accurate user groups and provisioning processes

wallarm

Silver Linings and Surprises #2 Drive for Efficiency

Drive for efficiency

- Frozen IT budgets
  - A tool deployed today is worth more than the one on the roadmap
    - Explore feature sets not previously prioritized
    - Expand on existing uses cases via cross team usage
- Increased workload on current systems/tools
  - Pay down tech debt.
  - Destroy False Positives or operationalize info gathering to determine FP faster

wallarm

Silver Linings and Surprises
#3 Distributed and Async Workflows

Support distributed and asynchronous creative workflows

- New tools implementation
  - Double down on remote collaboration
    - Architecture diagrams and planning
    - Less “shooting from the hip”
    - More documentation and planning for security architecture review

wallarm

Silver Linings and Surprises #4 Attack Volume

Increased attacks volume

- Attacks are not breaches
  - Hopefully
- Attacks are opportunities to learn and adapt
  - Signatures of attackers
  - Discover new attacks
- Consume the data and feed upstream tools and processes
  - Or have the information gathering and blocking tools be the same tool

wallarm

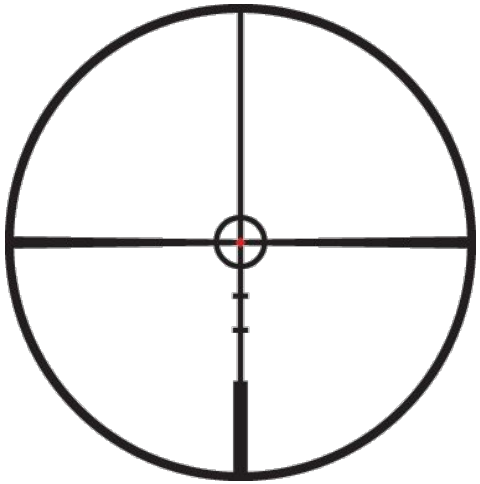
Survey results

It/InfoSec challenges in COVID19 times

wallarm

Attackers targets

- Corporate portals & social networks
- Corporate Docs management systems
- Vendors & contractors management tools
- Web interfaces for VPN’s
- E-mail systems web interface
- Corporate file archives



wallarm

Main application & API's risks during COVID-19

	Corporate portals & internal social networks	Dos management tools	Vendors & contractors management tools	Web interfaces for VPN's	E-mail systems web interface	Corporate file archives
SQL	High	High	High	Low	Low	High
XXE (XML-inj)	Medium	High	High	Low	Low	High
RCE/PTRAV	Medium	High	High	High	Low	High
XSS	High	High	High	High	High	High
CRLF & SMTP-inj	Low	Low	Low	Low	High	Low
Passwords fraud	Medium	Medium	High	Low	High	Medium
Date access breach	Medium	High	Medium	Low	Medium	High

High – incidents in 50+% surveyed companies
Medium – incidents in more than 10% of surveyed companies
Low – incident in less than 10% companies
Incident = confirmed application/API vulnerability attempt

wallarm

COVID-19 API/app security requirements

1. Fast scalability
2. Fast & timely implementation
3. Protecting API is as important as Applications security
4. False Positives ratio
5. Signal/Noise ratio. More attacks attempts make it difficult to detect critical cases

It’s **2020**, the time to **replace** your **yesterday’s WAF** to meet these 5 requirements

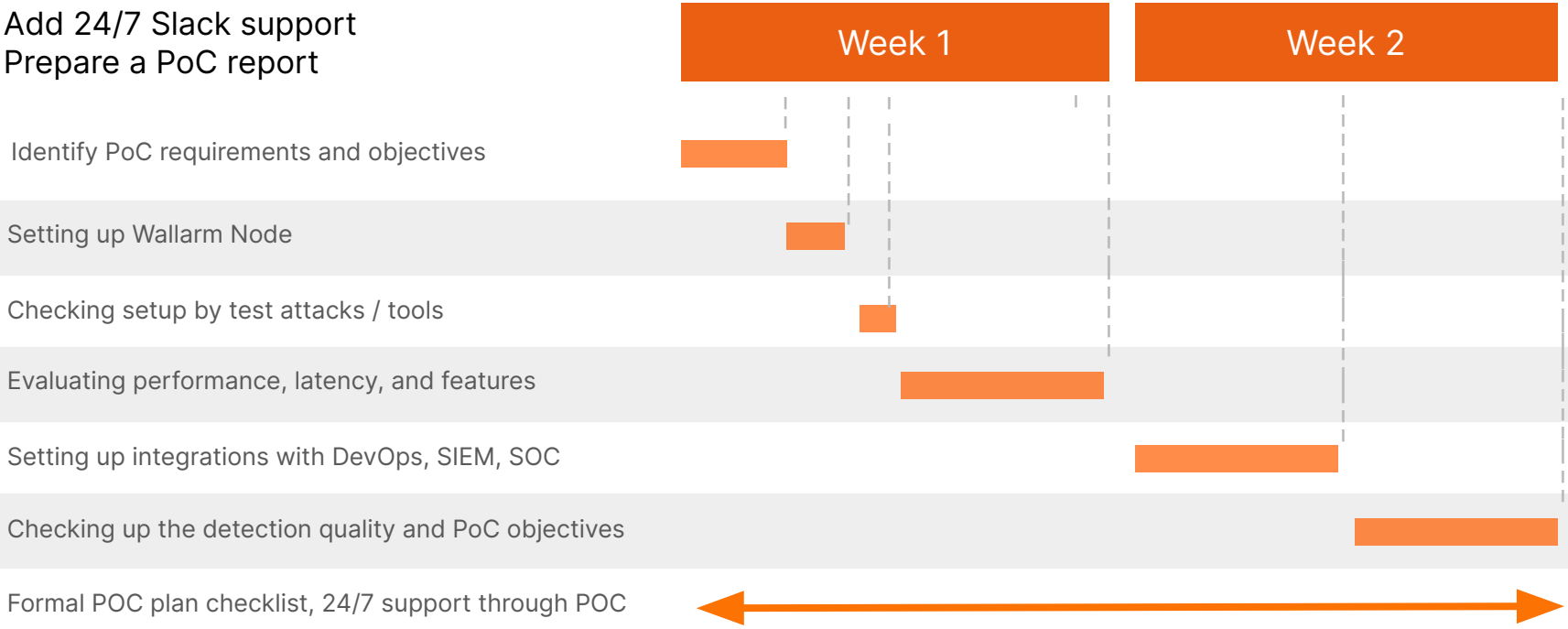
Replace yesterday's WAF

	Legacy WAF	Wallarm	COVID requirements
Deploy in cloud	Hard, not scalable	Up in 30 minutes	**Fast scalability**
API protection	Poor or zero	Built for it	**Protecting API and apps**
TCO	High. Requires tuning	Low. No tuning.	**False Positives ratio**
Blocking mode	Nightmare. Not usable.	Just works	**Signal/Noise ratio**
CI/CD readiness	False positives kill it	Doesn't break apps	**Fast implementation**
Vulns detection	Zero	Finds exploitable issues	**Signal/Noise ratio**

wallarm

Start your PoC today at wallarm.com

Add 24/7 Slack support
Prepare a PoC report



Contact us at request@wallarm.com to schedule your personal demo!

wallarm

Thank you!

Stay healthy
and secure with Wallarm

Contact us at request@wallarm.com to schedule your personal demo!