

www.pandoralabs.net



PANDORA SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

Website Security – Why It Matters
Isaac Sabas – isabas@pandoralabs.net



Expert advice. Experience advantage.

Proactive Security Solutions Through Cutting-Edge Research.

We are a security
software-as-a-service
(SaaS) company

1. What are websites to us?

How do we individually see the use and purpose of websites?

What does websites mean to us?

- Marketing
- Catalog/Brochure
- Blog/Content sharing
- E-commerce
- CRM
- *We understand that websites play a vital and important role towards our organization's success.*

2. Where the problem lies.

Why we are not taking security seriously

We did not factor in the security of our website.

We always think that we are the exception.

“I just use the our website to showcase our products. No confidential information is found there.”

“I don’t have any financial data on our website, what makes it so interesting for hackers?”

“I just write blogs and share my reviews. I don’t see why they want to hack my website.”

“I’m not a big fish online, and there are a lot other big fishes there. Why would they bother to hack me?”

“It’s just a website, what do hackers gain from it?”

Why hackers attacks you?

- Small to medium websites = Little to no security at all
- Malware
- Spam or DDoS
- Ruin reputation (defacement)
- Proxy
- *Your website is in a public domain.*
- *All of the attacks can happen to you without you even knowing*

3. Web Threats.

What are the web threats that exists?

OWASP Top 10

- SQL or Code Injections
- Broken Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Functional Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components w/ Known Vulnerabilities
- Unvalidated Redirects and Forwards

4. Existing solutions.

What are the existing solutions to help us defend against web threats?

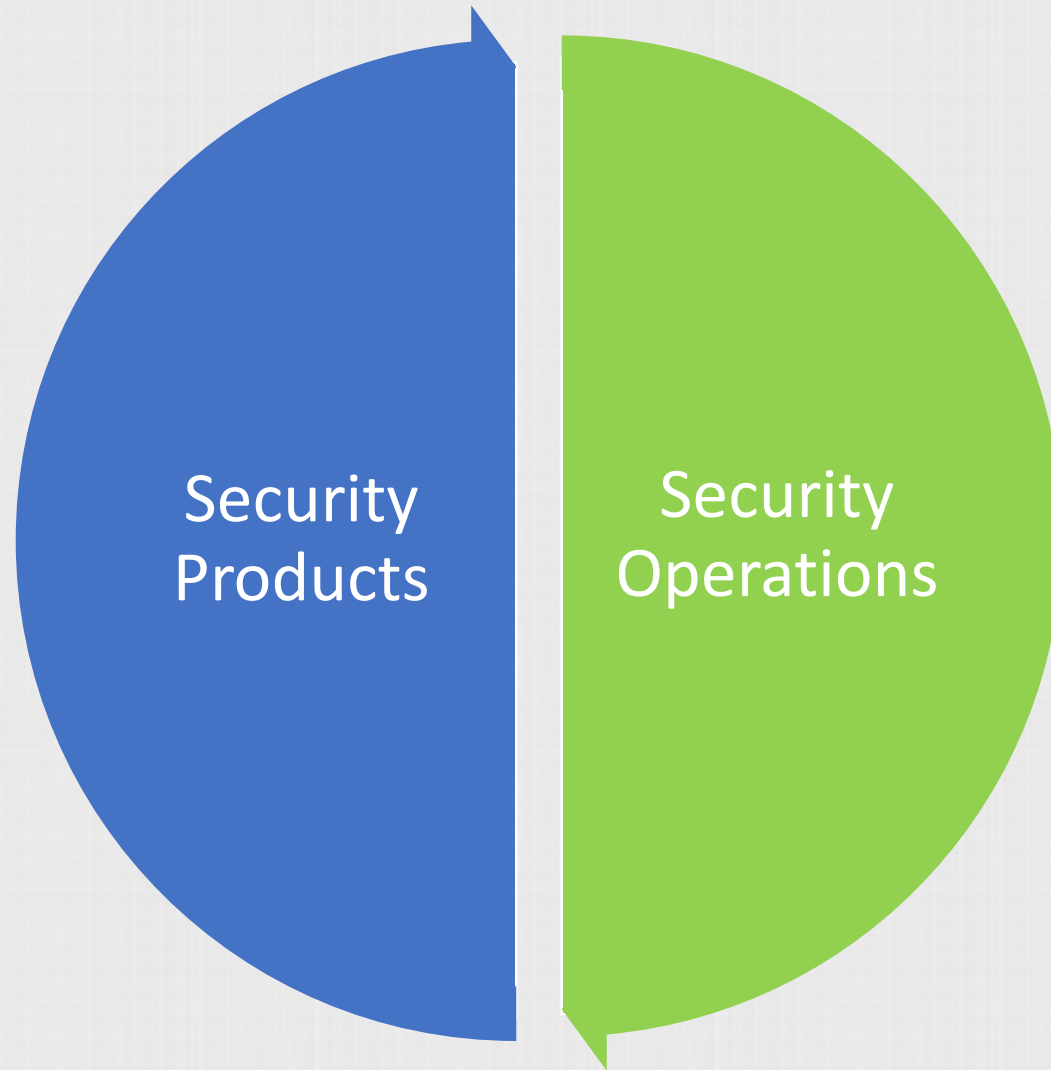
Security Products

- Self audit web applications – wpscan.org, etc.
- Security Plugins – each CMS usually have 2 or more options
- Web Application Firewall – ModSecurity, etc.
- Content Delivery Networks (CDN) – Cloudflare, Akamai

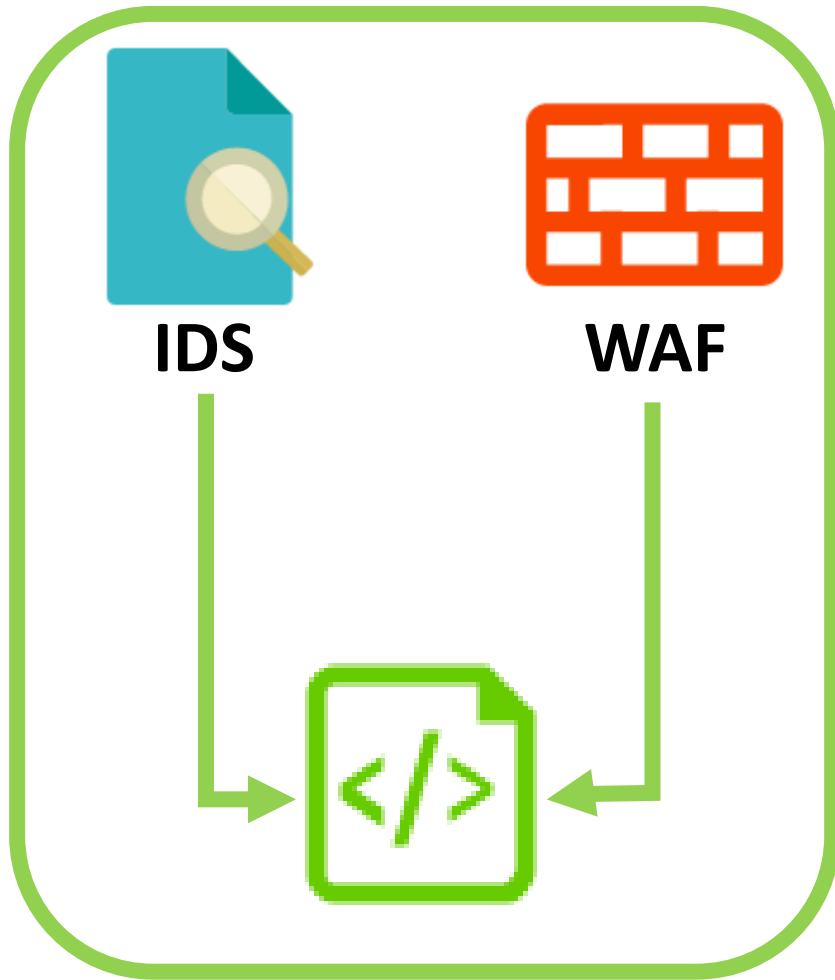
They all rely on you to operate and watch over it all the time.

5. Our solution – WebRanger™

Pandora WebRanger™ - 24x7 Web Proactive Protection



Security Products + Security Operations = Holistic Security



+



WebRanger™ + Pandora SOC = Holistic Security

ThreatScout™ Client Portal by Pandora Security Labs

Client Portal Navigation

- Client Portal Consoles
 - Dashboard
 - Events
 - Reports
- Client Portal Panel
 - User Settings

Dashboard Filter

Alert Information

Alert Risk Levels Emergency Alerts 11 <small>Last Alert Seen: 2015-02-20 11:28:07</small>	SIEM Information Total SIEM Events 160 <small>Last Event Seen: 2015-02-20 19:33:59</small>
High Alerts 7 <small>Last Alert Seen: 2015-02-20 10:58:57</small>	Resolved Alerts 45 <small>Last Alert Seen: 2015-02-20 10:58:57</small>
Medium Alerts 5 <small>Last Alert Seen: 2015-02-18 06:41:55</small>	Unresolved Alerts 6 <small>Last Alert Seen: 2015-02-20 11:30:53</small>
Low Alerts 28 <small>Last Alert Seen: 2015-02-20 11:30:53</small>	Events Per Second 0 <small>From events gathered 720 hours ago</small>

Client Disk Consumption

Alert Tickets

Ticket #	Alert Name	Alert Level	Alert Timestamp
116502	Low Impact PHPIDS Alert	LOW	2015-02-20 11:30
593044	Emergency Impact PHPIDS Alert	EMERGE...	2015-02-20 11:28
682777	Emergency Impact PHPIDS Alert	EMERGE...	2015-02-20 11:17
443269	Emergency Impact PHPIDS Alert	EMERGE...	2015-02-20 11:06
963967	Medium Impact PHPIDS Alert	MEDIUM	2015-02-10 10:41
277704	Emergency Impact PHPIDS Alert	EMERGE...	2015-01-28 11:08

Page 1 of 1 Displaying alerts 1 - 6 of 6

WebRanger™ monitored through ThreatScout™ SIEM



Let's launch a live attack!

www.pandoralabs.net



PANDORA SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

Website Security – Why It Matters
Isaac Sabas – isabas@pandoralabs.net