SWAP

For Better Web Security

cloudbric

Holes in your walls?

Hacker(s) exploit known vulnerabilities and use new methods of attacks, zero-day exploits, to carry out Advanced Persistent Threats (APTs) to infiltrate then extract sensitive information and sabotage networks without detection, and then return for more.

Traditional signature-based web application firewalls (WAFs) are designed to combat known threats; they cannot detect zero-day attacks that exploit modified or unknown attack patterns.

76% of Successful cyberattacks in 2018 were zero-day exploits[1]

64% of Companies attacked were hit again within 19 months[2]

79% of Companies say there's no guidance for APT protection[3]

cloudbric

Smarter in every way

Cloudbric's advanced logic-based detection engine in SWAP: Smart Web Application Protection uses Semantic Analysis[4] and Heuristic Analysis[5] in addition to traditional pattern matching techniques to detect known, unknown, and even modified web attacks with industry-leading accuracy. We protect your website and servers against web attacks, especially zero-day exploits, and advanced persistent threats in a fully automated and customizable setting.

SWAP's proprietary 27-rule set does not need constant updates of known signatures of attacks and the in-house deep learning A.I. 'VISION' evolves as more attack data is compiled, re-applying its learning results to achieve an even lower false positive rate.

cloudbric

Pinpoint precision

	Cloudbric SWAP	Cloudflare (US)	Shadan-kun (Japan)
True Positive Rate[6] (Higher is better)	92.50 %	75.31 %	77.50 %
False Positive Rate[7] (Lower is better)	2.19 %	6.88 %	10.63 %
False Negative Rate[7] (Lower is better)	7.50 %	24.69 %	22.50 %

False positive rates hurt businesses in more than one way[8]:

- Reduced sales and revenue
- Damaged reputation
- Lost customer relationships

Cloudbric VISION lowers the already best-in-class false positive rates :
Win back lost business opportunities with Cloudbric SWAP

cloudbric

Proactive protection

OWASP Top 10 Entries	2007	2010	2013	2017	cloudbric
Injection	A2	A1	A1	A1	Since 2005~
Broken Authentication[4]	A7	A3	A2	A2	
Sensitive Data Exposure[5]	A8	A7	A6[1]	A3	
XML External Entities (XXE)	-	-	-	A4[1]	
Broken Access Control[6]	A4	A4	A4	A5[2]	
Security Misconfiguration	-	A6	A5	A6	
Cross-Site Scripting (XSS)	A1	A2	A3	A7	
Insecure Deserialization	-	-	-	A8[1]	
Using Components with Known Vulnerabilities	-	-	A9[1]	A9	
Insufficient Logging & Monitoring	-	-	-	A10[1]	
Missing Function Level Access Control[7]	A10[8]	A8	A7[3]	-	
Cross-Site Request Forgery (CSRF)	A5	A5	A8	-	

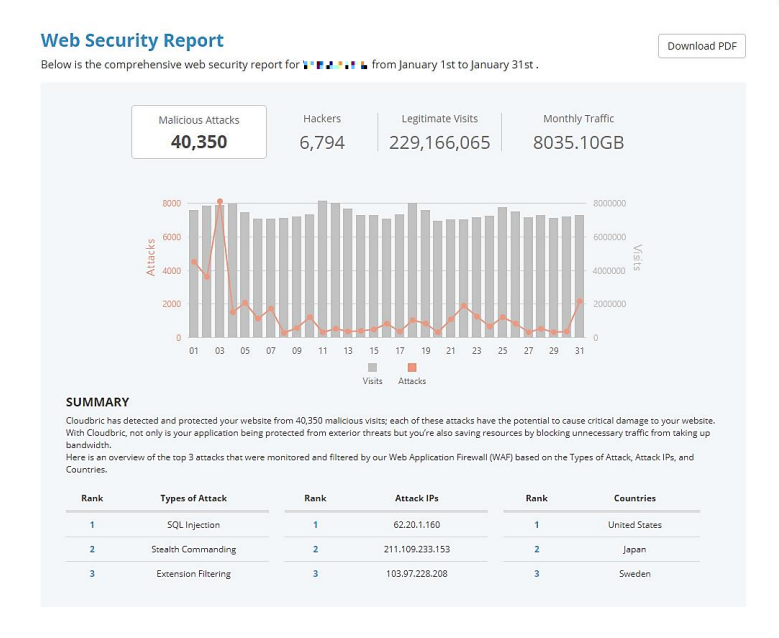
1: New Entries for Current Year
2: New Entries for Current Year –Merged from 2013 A4 and 2013 A7
3: New Entries for Current Year –Broadened definition from previous year
4: Renamed "Broken Authentication and Session Management" from 2010
5: Renamed "Insecure Cryptographic Storage" from 2010
6: Merged from "Insecure Direct Object Reference" from 2010
7: Renamed "Failure to Restrict URL Access" from 2010
8: Split "Broken Access Control" from T10 2004

The Open Web Application Security Project releases a list of the most critical web application security risks every 3-4 years.[9]

Cloudbric SWAP's advanced logic has been providing protection against security risks even before they were prevalent issues.[10]

cloudbric

Keep your operations simple



Cloudbric provides an intuitive dashboard that tracks malicious attack attempts, monthly traffic, most common types of web attacks, and a list of dangerous IPs to blacklist.

In addition, all partners have access to private admin console to help manage client accounts and 24/7 technical support, including on-hand engineers dedicated to keeping SWAP instances and websites online.

SWAP, provided as a virtual image, can be installed inside the user's server infrastructure (dedicated, cloud, or VPS) or as dedicated instances through Cloudbric's vast data center networks. OEM licensed white labeling is also available for hosting/service providers who want to provide SWAP as an add-on service for their end-users.

cloudbric

Trusted around the world

Cloudbric, with more than 20 years of industry experience, is recognized & trusted by more than 10,000 enterprises and small businesses spanning 25+ countries. We operate twenty-eight dedicated service regions to protect private companies and public institutions in finance, commerce, healthcare, security, communications, and more.

cloudbric

Contacts

Albert Oh
Senior Business Development Manager
email albert@cloudbric.com
office +82 2 2125 6511
mobile +82 10 3389 6488

for more information on Cloudbric SWAP
and our becoming our partner

cloudbric

Appendix

References

1: Ponemon Institute (2018, October). 2018 State of Endpoint Security Risk. Retrieved from https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

2. FireEye Mandiant Services (2019). M-Trends 2019 Special Report. Retrieved from https://content.fireeye.com/m-trends/rpt-m-trends-2019

3. ISACA (2012). Advanced Persistent Threat Awareness. Retrieved from https://www.trendmicro.it/media/misc/apt-survey-report-en.pdf

6. Results via WAFER: a WAF performance testing software (2018). Test patterns consist of OWASP core rule sets, exploit DB patterns, and other common attack patterns

8. The Payers (2018). False positives hurt your business more than you think. Retrieved from https://thepaypers.com/expert-opinion/false-positives-hurt-your-business-more-than-you-think--773673

9. OWASP Top Ten (2020) Retrieved February 02, from https://owasp.org/www-project-top-ten/

10. Penta Security Systems Inc. (2006, November). WAPPLESECURITY Gateway Introduction. Available upon request.

Glossary

4 Semantic Analysis: A method of detecting web attacks in which a logic engine analyzes the syntax structure of each incoming and outgoing web packet to check for conditions according to the logic developed by Cloudbric security engineers.

5 Heuristic Analysis: A method of detecting web attacks by comparing heuristic patterns of incoming traffic packets against previously known attacks; this differs from the typical Pattern Matching method—as heuristic analysis would be able to detect and block out modified versions of known patterns based on probability evaluation.

7 False Positives and False Negatives: False positive error, more commonly known as ‘false alarm’ indicates an error in which a test result improperly indicates presence or a condition; think ‘The Boy Who Cried Wolf.’ In case of web protection, falsely identifying safe traffic as malicious web attack would be considered a false positive. False negative error is a test result that indicates that a condition that does not hold, when in fact it does. In case of web protection service, letting a known malicious attack attempt pass through a detection engine unnoticed would be considered a false negative.

cloudbric