

ECB ACTION PLAN · APPLICATION LAYER

ANSWERING THE ECB LETTER? RAVEN HELPS YOU STOP UNKNOWN ATTACKS.

Most of your code is public. Attackers are using AI to find the exploits. No CVE, no warning. **Raven prevents the exploits at runtime, with or without a CVE.**



/ 01 WHAT THE ECB EXPECTS A resourced plan with owners and timelines

 Exposed assets	 Faster remediation	 Monitoring	 Third-party readiness	 Layered defenses	 Recovery
--	--	--	---	--	--

/ 02 PUT RUNTIME PREVENTION IN YOUR PLAN

Watch every library at runtime to address all six ECB expectations at the application layer.

- ✓ No CVE required**
 Library-level policies stop abnormal behavior before a CVE exists.
 **MONITORING**  **EXPOSED ASSETS**
- ✓ No code changes. No patching.**
 Protection in production now; fixes follow your plan's timeline.
 **FASTER REMEDIATION**
 **LAYERED DEFENSES**
- ✓ Code-level evidence**
 Exact library, function and call path for AppSec and the SOC.
 **THIRD-PARTY READINESS**
 **RECOVERY**

YOUR APPLICATION AT RUNTIME
● REC

 OpenSSL	 libxml2	 Log4j	 Jackson
 Spring	 Struts	 TensorFlow	 PyTorch
 Django	 Jinja2	 Express	 Lodash

Log4j and Jinja2 were both exploited with no CVE assigned. Raven stopped both at runtime.

Raven watches every library at runtime. Sees the exploit. Prevents it. No slowdowns. No patching.

SEE HOW RAVEN PREVENTS EXPLOITS

No performance impact · All languages · 5-minute install

[Learn more at raven.io](https://raven.io) →