Hitting Above The Security Mendoza Line
Ed Bellis, CEO Risk I/O
Nice To Meet You

About Me

CoFounder Risk I/O
Former CISO Orbitz
Contributing Author
Beautiful Security
CSO Magazine/Online Writer
InfoSec Island Blogger

About Risk I/O

Data-Driven Vulnerability Management as a Service
DataWeek 2012 Top Security Innovator
3 Startups to Watch - Information Week
16 Hot Startups - eWeek
About Mario

Played for Pirates, Rangers & Mariners

Played MLB for 9 Seasons

Lifetime Batting Avg: .214, 4HR, 101 RBI

Failed to bat .200 5 times
The Security Mendoza Line

Wouldn’t it be nice if we had something that helped us divide who we considered “Amateur” and who we considered “Professional”?

Enter The Security Mendoza Line

Alex Hutton came up with original concept of the Security Mendoza Line

http://riskmanagementinsight.com/riskanalysis/?p=294
HD Moore’s Law

Josh Corman expands the Security Mendoza Line

“You must be this tall to ride this tall this tall this tall”

“Compute power grows at the rate of doubling about every 2 years”

“Casual attacker power grows at the rate of Metasploit”
A Difficult Task

Nearly 2K MSF Exploits

ExploitDB > 18K Exploits
Point ➔ Click ➔ Pwn
A Data Driven Approach
Out Scripting the Kiddies

Fighting Automation with Automation

Netflix/
SimianArmy
Github

Avg: .200
Context Matters

Attack
Path data analysis

Avg: .220
Context Matters

Mitigating Controls

- Firewalls / ACLs
- IPS
- WAF
- MFA
- Other

Avg: .240
Context Matters

Honeypot, WAF & IDS data logs! logs! logs!

Measuring Likelihood

Avg: .260
Broader Context

Targets of Opportunity?

\[
\text{My(vuln posture X other threat activity)} / (\text{other vuln posture X other threat activity})
\]

Avg: .280
Beyond Info Sharing

Model Sharing

ALL Star!
Avg: .300
A Quick Side Note

CVE Trending Analysis

Gunnar’s Debt Clock

<table>
<thead>
<tr>
<th>Year</th>
<th>Developers</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>CGI, PERL</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1997</td>
<td>ASP, JSP</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1998</td>
<td>EJB, J2EE, DCOM</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1999</td>
<td>SOAP, XML</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>2001</td>
<td>Rest, SOA</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>2003</td>
<td>Web 2.0</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>2007</td>
<td>Cloud Computing</td>
<td>Network firewalls, SSL</td>
</tr>
</tbody>
</table>
Q & A

follow us

the blog
http://blog.risk.io/

twitter
@ebellis
@riskio

And one more thing....

We’re Hiring! https://www.risk.io/jobs