




PCTY2011



Pulse Comes to You

Optimising the World's Infrastructure



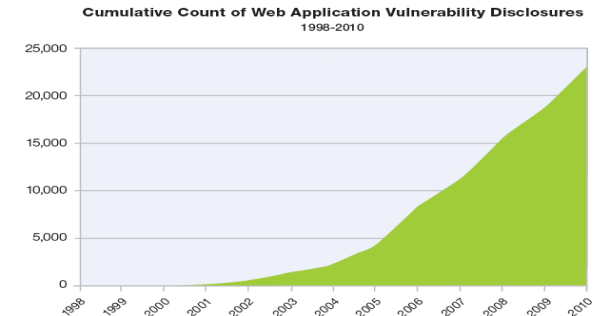
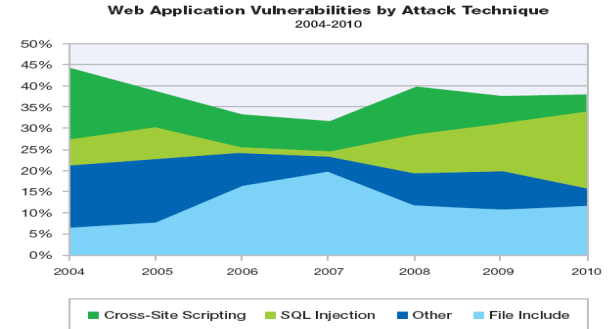
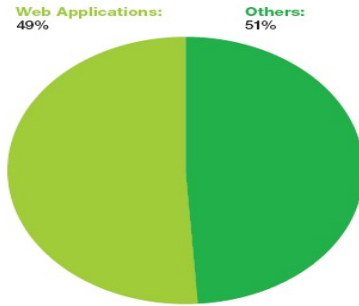
Application vulnerabilities - and the virtual patch

Gareth O Sullivan
IBM Rational Security Tech Sales Lead EMEA

Web App Vulnerabilities Continue to Dominate

- Nearly half (**49%**) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2010



The Costs from Security Breaches are Staggering

**285 MILLION RECORDS
COMPROMISED IN 2008**

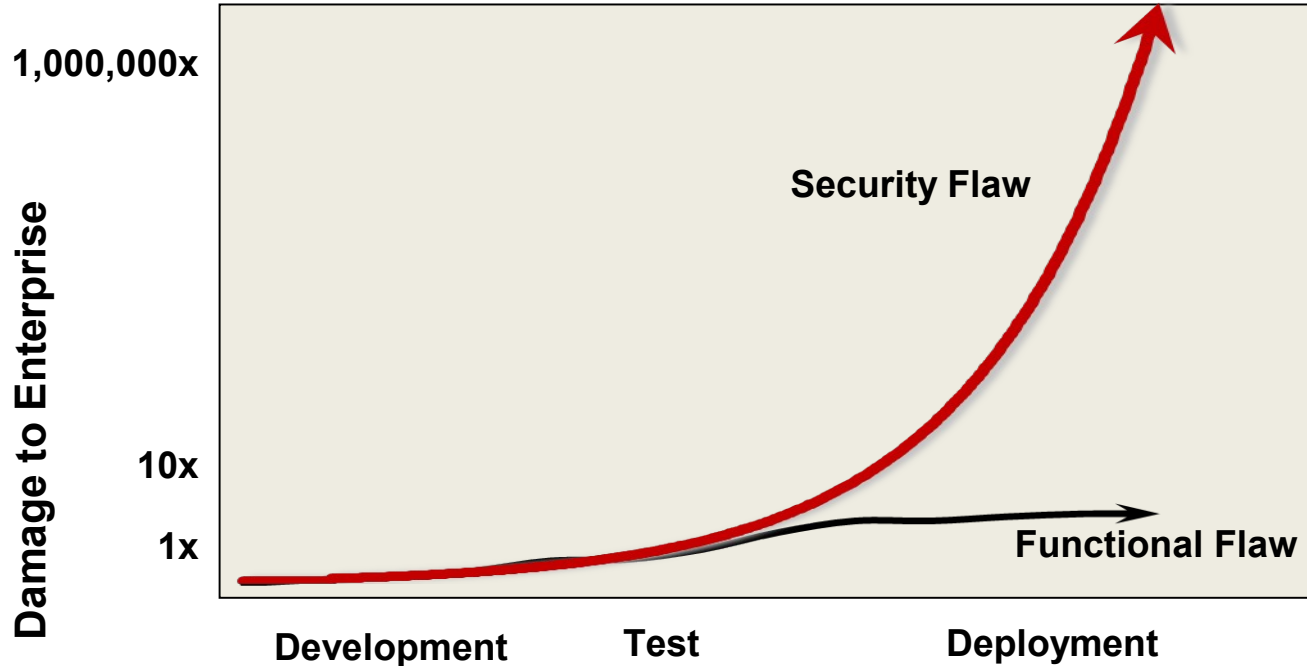
Verizon 2009 data
Breach
Investigations
Report

**\$204 COST PER
COMPROMISED
RECORD**

Ponemon 2009-
2010 Cost of a data
Breach Report

**TRANSLATES TO \$58.1B
COST TO CORPORATIONS**

Sources of Security Breach Costs



Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

More Justification for Application Security Action

99.9% of records were compromised from servers and applications

81% of organizations subject to PCI had not been found compliant prior to the breach

79% of compromised records were compromised using Web applications as the attack pathway



Verizon 2009 data Breach Investigations Report

Action:

- Adopt application security measures
- Address compliance mandates with industry regulations (such as PCI-DSS, GLBA, HIPAA, FISMA, NERC, etc)

Why are Web Applications so Vulnerable?

- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software for a Smarter Planet
- Network scanners won't find application vulnerabilities and firewalls/IPS don't block application attacks



Volumes of applications continue to be deployed that are riddled with security flaws...

...and are non compliant with industry regulations

Pre-empt Costly Risk Mitigation – Become Secure, by Design

Customer Speak!

Reduce today's **most significant area** of risk by **adopting a cost effective** and thorough application security program



"We have more of our business supported by our web presence – we can't afford the business risk of deploying unsecured applications and services"

Embed security early into the software delivery process to **enable on time and on budget delivery** of secure applications



"Embracing security in development allowed us to get ahead of schedule disruption and increased costs from security acceptance testing"

Establish a security blueprint to **create and maintain security governance, manage risk and ensure compliance**



"IBM has recognized this trend and has created comprehensive security packages that leverage various products to provide for multiple layers of security to customers"

Make Applications Secure, by Design

Design Phase

- Consideration is given to security requirements of the application
- Issues such as required controls and best practices are documented on par with functional requirements

Development Phase

- Software is checked during coding for:
 - Implementation error vulnerabilities
 - Compliance with security requirements

Build & Test Phase

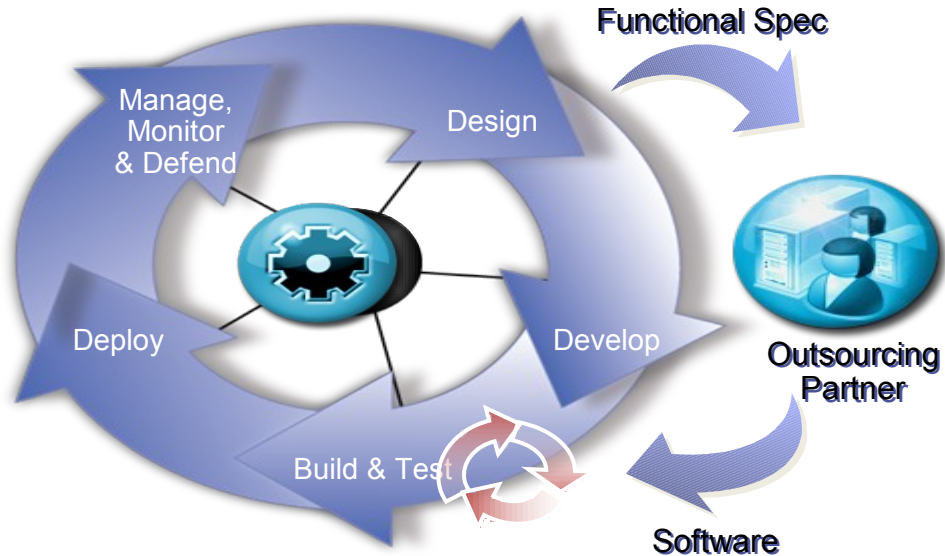
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

Operational Phase

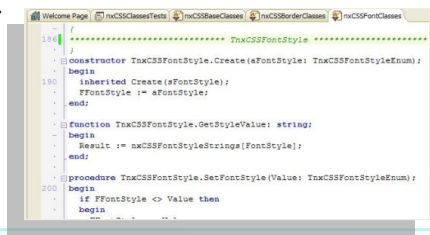
- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks



Security Testing Technologies... Combination Drives Greater Solution

Static Code Analysis (Whitebox)

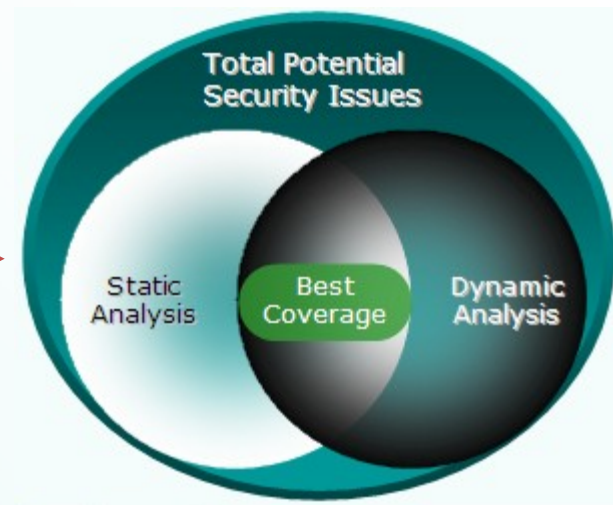
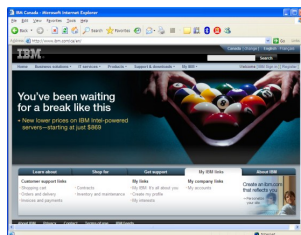
- Scanning source code for security issues



```
184 /
185 /
186 /
187 /
188 /
189 /
190 /
191 /
192 /
193 /
194 /
195 /
196 /
197 /
198 /
199 /
200 /
201 /
202 /
203 /
204 /
205 /
206 /
207 /
208 /
209 /
210 /
211 /
212 /
213 /
214 /
215 /
216 /
217 /
218 /
219 /
220 /
221 /
222 /
223 /
224 /
225 /
226 /
227 /
228 /
229 /
230 /
231 /
232 /
233 /
234 /
235 /
236 /
237 /
238 /
239 /
240 /
241 /
242 /
243 /
244 /
245 /
246 /
247 /
248 /
249 /
250 /
251 /
252 /
253 /
254 /
255 /
256 /
257 /
258 /
259 /
260 /
261 /
262 /
263 /
264 /
265 /
266 /
267 /
268 /
269 /
270 /
271 /
272 /
273 /
274 /
275 /
276 /
277 /
278 /
279 /
280 /
281 /
282 /
283 /
284 /
285 /
286 /
287 /
288 /
289 /
290 /
291 /
292 /
293 /
294 /
295 /
296 /
297 /
298 /
299 /
300 /
301 /
302 /
303 /
304 /
305 /
306 /
307 /
308 /
309 /
310 /
311 /
312 /
313 /
314 /
315 /
316 /
317 /
318 /
319 /
320 /
321 /
322 /
323 /
324 /
325 /
326 /
327 /
328 /
329 /
330 /
331 /
332 /
333 /
334 /
335 /
336 /
337 /
338 /
339 /
340 /
341 /
342 /
343 /
344 /
345 /
346 /
347 /
348 /
349 /
350 /
351 /
352 /
353 /
354 /
355 /
356 /
357 /
358 /
359 /
360 /
361 /
362 /
363 /
364 /
365 /
366 /
367 /
368 /
369 /
370 /
371 /
372 /
373 /
374 /
375 /
376 /
377 /
378 /
379 /
380 /
381 /
382 /
383 /
384 /
385 /
386 /
387 /
388 /
389 /
390 /
391 /
392 /
393 /
394 /
395 /
396 /
397 /
398 /
399 /
400 /
401 /
402 /
403 /
404 /
405 /
406 /
407 /
408 /
409 /
410 /
411 /
412 /
413 /
414 /
415 /
416 /
417 /
418 /
419 /
420 /
421 /
422 /
423 /
424 /
425 /
426 /
427 /
428 /
429 /
430 /
431 /
432 /
433 /
434 /
435 /
436 /
437 /
438 /
439 /
440 /
441 /
442 /
443 /
444 /
445 /
446 /
447 /
448 /
449 /
450 /
451 /
452 /
453 /
454 /
455 /
456 /
457 /
458 /
459 /
460 /
461 /
462 /
463 /
464 /
465 /
466 /
467 /
468 /
469 /
470 /
471 /
472 /
473 /
474 /
475 /
476 /
477 /
478 /
479 /
480 /
481 /
482 /
483 /
484 /
485 /
486 /
487 /
488 /
489 /
490 /
491 /
492 /
493 /
494 /
495 /
496 /
497 /
498 /
499 /
500 /
501 /
502 /
503 /
504 /
505 /
506 /
507 /
508 /
509 /
510 /
511 /
512 /
513 /
514 /
515 /
516 /
517 /
518 /
519 /
520 /
521 /
522 /
523 /
524 /
525 /
526 /
527 /
528 /
529 /
530 /
531 /
532 /
533 /
534 /
535 /
536 /
537 /
538 /
539 /
540 /
541 /
542 /
543 /
544 /
545 /
546 /
547 /
548 /
549 /
550 /
551 /
552 /
553 /
554 /
555 /
556 /
557 /
558 /
559 /
560 /
561 /
562 /
563 /
564 /
565 /
566 /
567 /
568 /
569 /
570 /
571 /
572 /
573 /
574 /
575 /
576 /
577 /
578 /
579 /
580 /
581 /
582 /
583 /
584 /
585 /
586 /
587 /
588 /
589 /
590 /
591 /
592 /
593 /
594 /
595 /
596 /
597 /
598 /
599 /
600 /
601 /
602 /
603 /
604 /
605 /
606 /
607 /
608 /
609 /
610 /
611 /
612 /
613 /
614 /
615 /
616 /
617 /
618 /
619 /
620 /
621 /
622 /
623 /
624 /
625 /
626 /
627 /
628 /
629 /
630 /
631 /
632 /
633 /
634 /
635 /
636 /
637 /
638 /
639 /
640 /
641 /
642 /
643 /
644 /
645 /
646 /
647 /
648 /
649 /
650 /
651 /
652 /
653 /
654 /
655 /
656 /
657 /
658 /
659 /
660 /
661 /
662 /
663 /
664 /
665 /
666 /
667 /
668 /
669 /
670 /
671 /
672 /
673 /
674 /
675 /
676 /
677 /
678 /
679 /
680 /
681 /
682 /
683 /
684 /
685 /
686 /
687 /
688 /
689 /
690 /
691 /
692 /
693 /
694 /
695 /
696 /
697 /
698 /
699 /
700 /
701 /
702 /
703 /
704 /
705 /
706 /
707 /
708 /
709 /
710 /
711 /
712 /
713 /
714 /
715 /
716 /
717 /
718 /
719 /
720 /
721 /
722 /
723 /
724 /
725 /
726 /
727 /
728 /
729 /
730 /
731 /
732 /
733 /
734 /
735 /
736 /
737 /
738 /
739 /
740 /
741 /
742 /
743 /
744 /
745 /
746 /
747 /
748 /
749 /
750 /
751 /
752 /
753 /
754 /
755 /
756 /
757 /
758 /
759 /
760 /
761 /
762 /
763 /
764 /
765 /
766 /
767 /
768 /
769 /
770 /
771 /
772 /
773 /
774 /
775 /
776 /
777 /
778 /
779 /
780 /
781 /
782 /
783 /
784 /
785 /
786 /
787 /
788 /
789 /
790 /
791 /
792 /
793 /
794 /
795 /
796 /
797 /
798 /
799 /
800 /
801 /
802 /
803 /
804 /
805 /
806 /
807 /
808 /
809 /
810 /
811 /
812 /
813 /
814 /
815 /
816 /
817 /
818 /
819 /
820 /
821 /
822 /
823 /
824 /
825 /
826 /
827 /
828 /
829 /
830 /
831 /
832 /
833 /
834 /
835 /
836 /
837 /
838 /
839 /
840 /
841 /
842 /
843 /
844 /
845 /
846 /
847 /
848 /
849 /
850 /
851 /
852 /
853 /
854 /
855 /
856 /
857 /
858 /
859 /
860 /
861 /
862 /
863 /
864 /
865 /
866 /
867 /
868 /
869 /
870 /
871 /
872 /
873 /
874 /
875 /
876 /
877 /
878 /
879 /
880 /
881 /
882 /
883 /
884 /
885 /
886 /
887 /
888 /
889 /
890 /
891 /
892 /
893 /
894 /
895 /
896 /
897 /
898 /
899 /
900 /
901 /
902 /
903 /
904 /
905 /
906 /
907 /
908 /
909 /
910 /
911 /
912 /
913 /
914 /
915 /
916 /
917 /
918 /
919 /
920 /
921 /
922 /
923 /
924 /
925 /
926 /
927 /
928 /
929 /
930 /
931 /
932 /
933 /
934 /
935 /
936 /
937 /
938 /
939 /
940 /
941 /
942 /
943 /
944 /
945 /
946 /
947 /
948 /
949 /
950 /
951 /
952 /
953 /
954 /
955 /
956 /
957 /
958 /
959 /
960 /
961 /
962 /
963 /
964 /
965 /
966 /
967 /
968 /
969 /
970 /
971 /
972 /
973 /
974 /
975 /
976 /
977 /
978 /
979 /
980 /
981 /
982 /
983 /
984 /
985 /
986 /
987 /
988 /
989 /
990 /
991 /
992 /
993 /
994 /
995 /
996 /
997 /
998 /
999 /
1000 /
```

Dynamic Analysis (Blackbox)

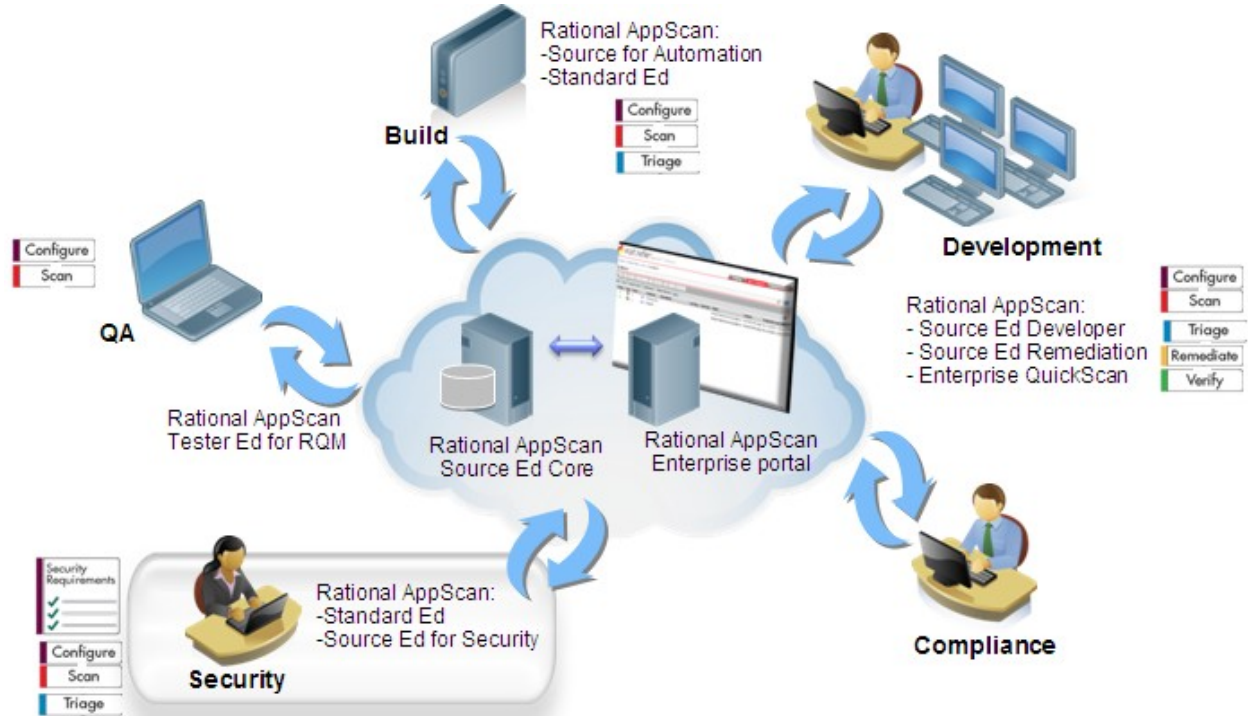
- Performing security analysis of a compiled application



Application security scanning

Functions:

- Security Requirements
 - ✓
 - ✓
 - ✓
- Configure
- Scan
- Triage
- Remediate
- Verify



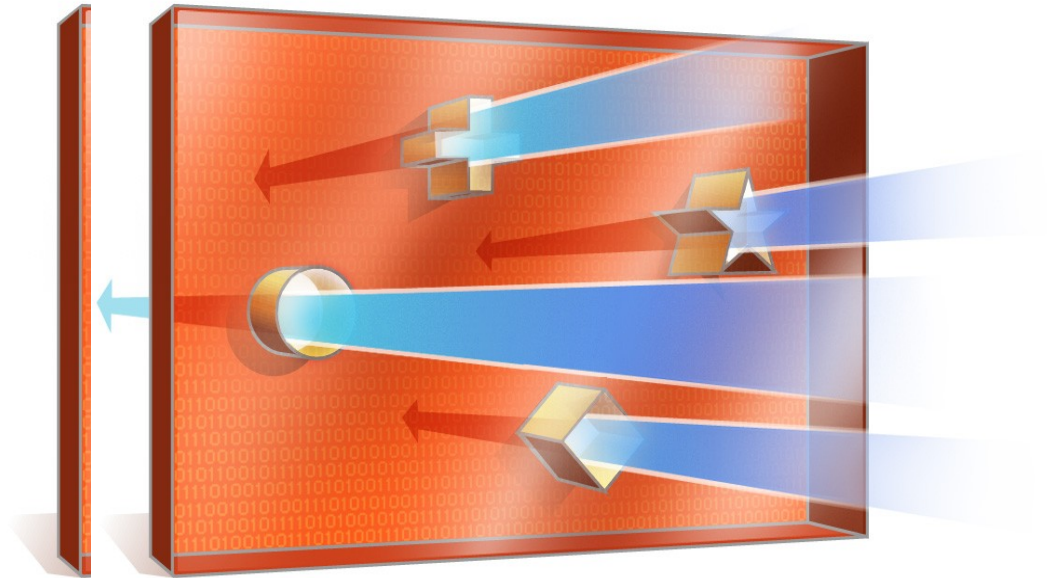
Application development meets service management

So what happens when I locate a vulnerability, and the application owner tells me we can't patch the system for 3 months!



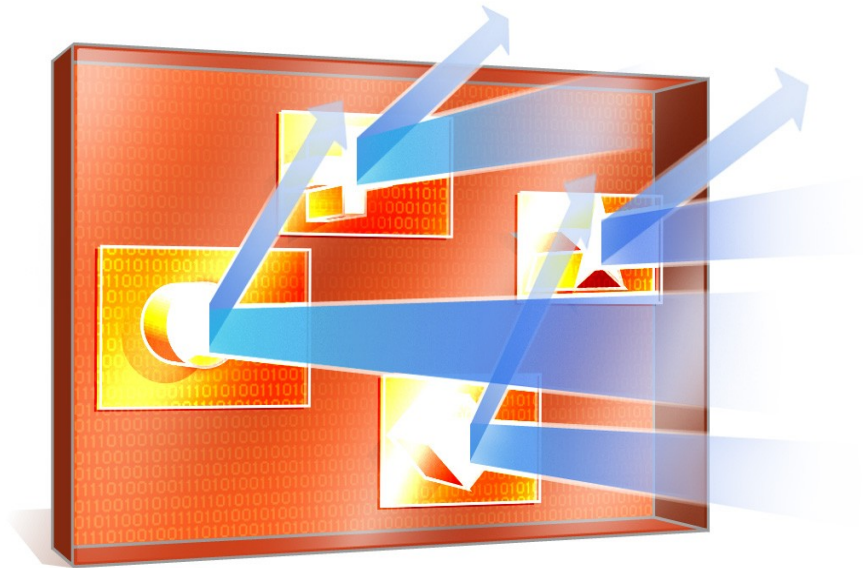
All Threats Exploit Some Vulnerability

Internet threats take advantage of a vulnerability in the Operating system, application or network infrastructure

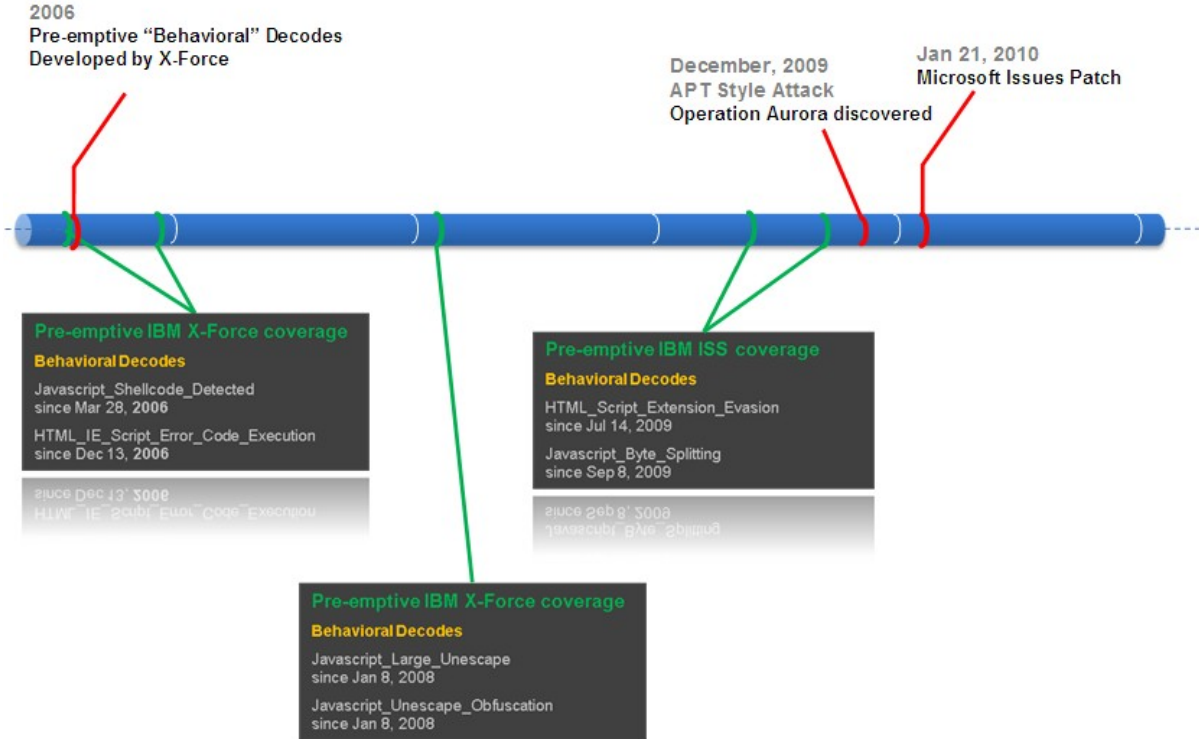


Preemptive security works by providing a temporary shield or “**virtual patch**” for known vulnerabilities

- Provides 0-day protection by preventing the vulnerability from being exploited
- Blocks all variations of the threat
- Doesn't rely on “signatures”
- Eliminates emergency patching
- Removes the risk that a patch will break something
- Enables patches to be applied during normal maintenance windows



Ahead of the Threat: Operation Aurora



Application development meets service management

Build Secure Web Applications

- Secure code development
- Identify vulnerabilities and malware
- Actionable information to correct the problems

Protect Web applications from potential attacks

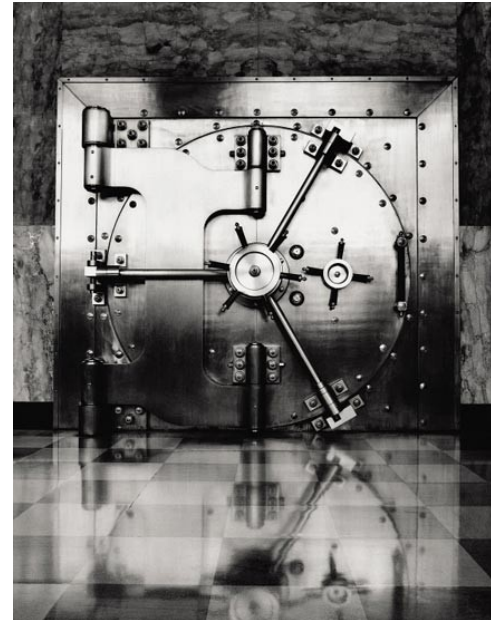
- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

Manage Secure Web Applications

- Single management console for vulnerabilities, events and blocking policies

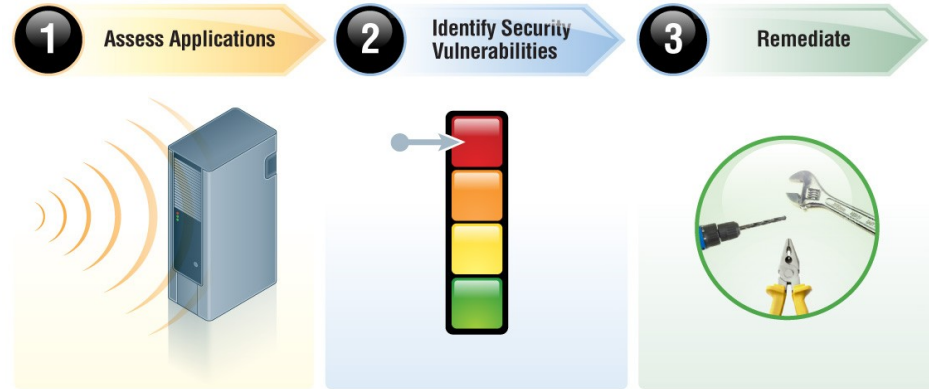
Managing secure web applications

- Drive intelligent security with integrated single console for AppScan and Proventia IPS
- Centrally manage vulnerabilities, IPS blocking/alerting policies and security events from a single dashboard
- Correlate vulnerabilities with security events & attacks blocked
- Consolidate reporting for compliance requirements and improved management
- Build and apply security policies to block threats specific to your vulnerabilities



Summary

- Reduce costs
- Decrease risk
- Speed time to market for applications
- Automate manual tasks





Q&A



X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security. Find out more at <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>



Thank
You