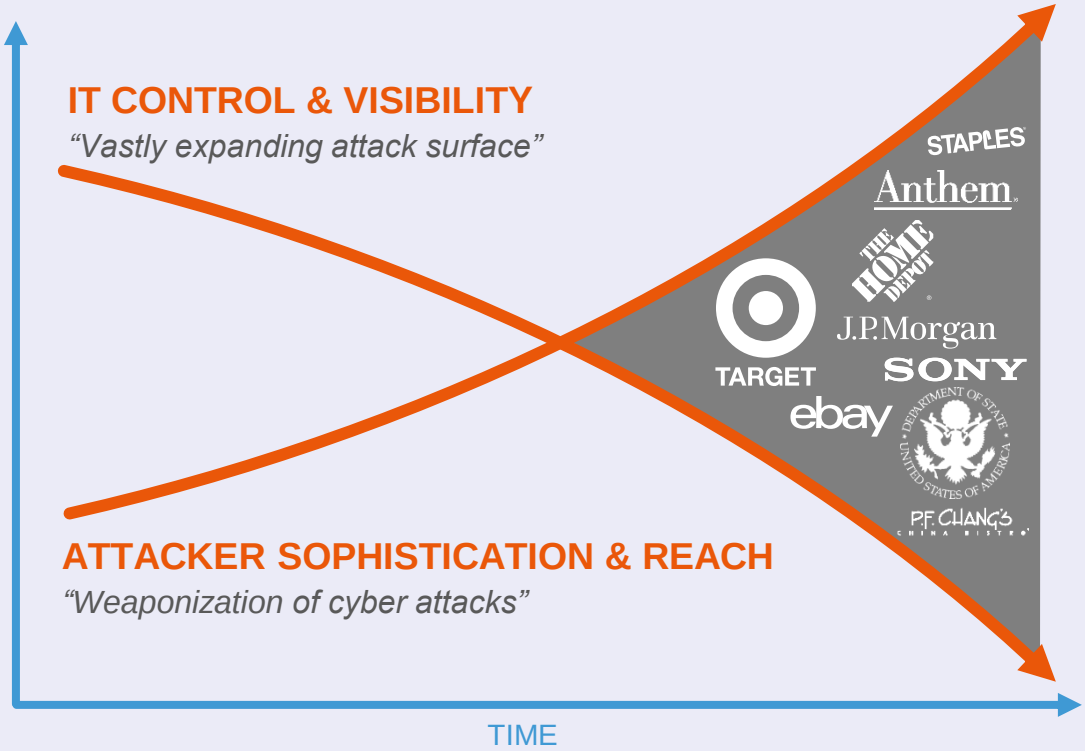
Engineering better security

OWASP 中国
The Open Web Application Security Project

SECURITY DATA & ANALYTICS


IT CONTROL & VISIBILITY
"Vastly expanding attack surface"
ATTACKER SOPHISTICATION & REACH
"Weaponization of cyber attacks"
TIME
STAPLES
Anthem
THE HOME DEPOT
TARGET
J.P.Morgan
SONY
ebay
DEPARTMENT OF STATE
UNITED STATES OF AMERICA
P.F. CHANG'S

控制安全风险——漏洞管理系统

Know Your Network
了解您的网络

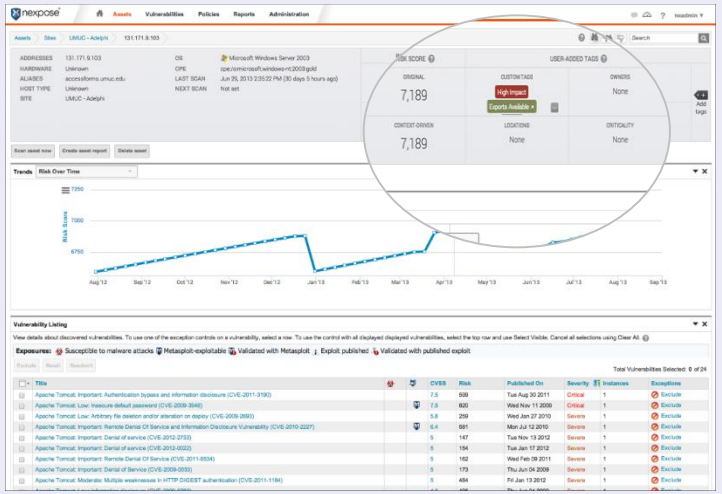
Manage Risk Effectively
有效管理风险

Simplify Your Compliance
简单处理合规需求

了解业务需求

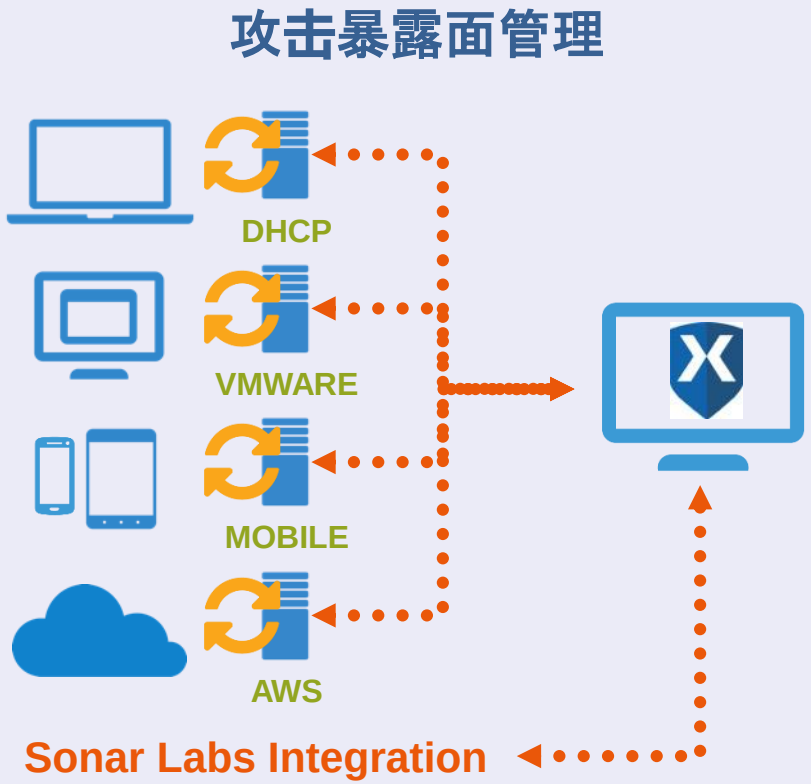
- 自动归类
- 定义资产的重要性
- 设定修补和资产的责任人

RealContext™



自适应的安全

- 自动发现新的资产加入网络
- 跟踪网络和信息资产的风险变化
- 了解所有外部资产



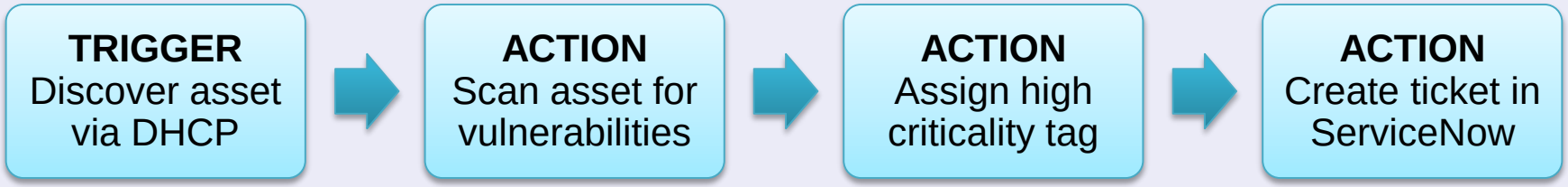
自适应安全

- 自动扫描整个网络的情况
- 自动触发扫描任务，基于设定的搜索条件，比如CVSS分数。
- 不需要人工干预

Emergent Threats

Zero Day

自动工作流



When new asset is discovered

If asset has risk score > 500

If asset is Windows server

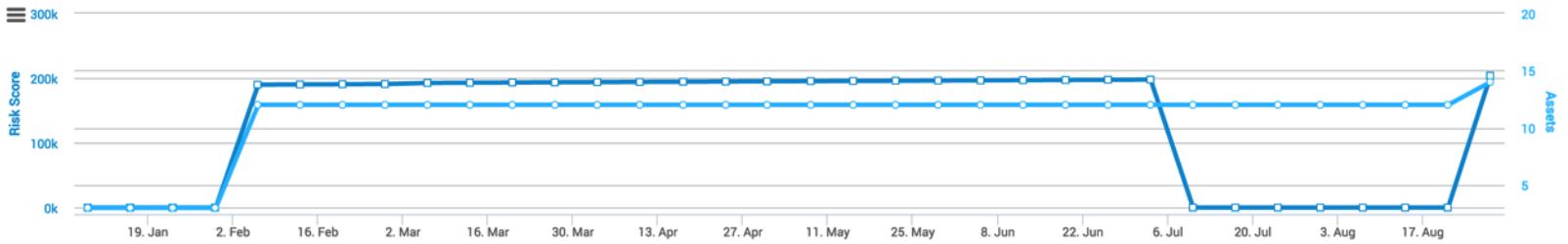
nexpose

nxadmin

ITEMS

RISK AND ASSETS OVER TIME

View by site or asset group



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
14 ▲ (was 12)	203,642 ▲ (was 0.0)	scan set to restart ▲ 67,742 (was N/A)	N/A	10.4.30.246 ▲ 55,132 (was N/A)	N/A

SITES

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
scan set to restart	3	220	67,742	ub1204-6aeu0-jy.dev.lax.rapid7.com	Static	Scheduled scan finished on Fri, Aug 28th, 2015			
site with one time schedule	0	0	0.0	Local scan engine	Static	Not scanned			
non default scan template - schedule hourly	3	0	0.0	ub1204-6aeu0-jy.dev.lax.rapid7.com	Static	Scheduled scan finished on Fri, Aug 28th, 2015			
paused scan set to restart	0	0	0.0	Local scan engine	Static	Scheduled scan paused on Thu, Jan 8th, 2015			

Showing 1 to 4 Rows per page: 10 1 of 1

CREATE SITE

New Intuitive User Interface

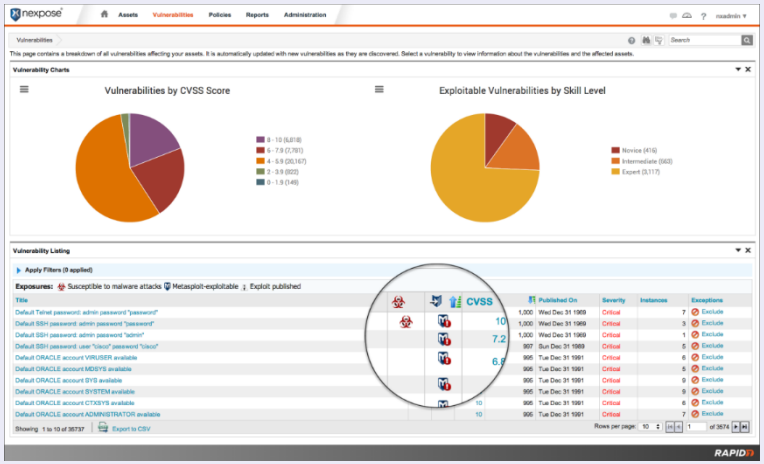
paused scan set to restart	Scheduled	1/8/2015 2:37 PM	3	0	1 minute	1/8/2015 2:38 PM	Local scan engine	Paused by system because the scan duration has been met.	
paused scan set to resume	Scheduled	8/28/2015 1:37 AM	1	0	12 hours, 1 minute	8/28/2015 1:38 PM	2 scan engines	Paused by system because the scan duration has been met	

SCAN NOW

漏洞验证n_MetaSploit Pro

- 安全地漏洞验证机制
- 专注在已知的安全风险
- 闭环的漏洞管理

Validate with Metasploit



TRADITIONAL VULNERABILITY MANAGEMENT

漏洞告警列表

ID	Title	Occurrences
MS05-43	Microsoft Windows DCOM RPCSS Service Vulnerabilities	14352
MS04-61	Microsoft Windows DCOM RPC Interface Buffer Overrun Vuln	11253
MS05-72	Microsoft Windows ASN.1 Library Integer Handling	2456
MS03-32	Windows TCP/IP Remote Code Execution	522
AP04-32	Apache Tomcat Directory Traversal	414
AW01-34	APR-util Library Integer Overflow	255
AP04-16	Apache 1.3 and 2.0 Web Server	116
FT01	ProFTPD 1.3 2xc2 and Prior_mod SQL Injection	98
VZ02	OpenVZ Multiple Vulnerabilities	64
HPJ01	HP NonStop Servers and Java	55
HW08	Huawei Multiple Device Bypass	32
MS04-47	Microsoft Messenger Service Buffer Overrun Vulnerability	28
RHL013	Red Hat Linux Instance 1.3 Multiple Vulnerabilities	28
PP32-1	Plug and Play Remote Access Vulnerability	19
SMOSL1	SQL_mod remote Once Single Access	18

清晰、直观、可操作

合规分析和报告

- 自定义所需要的报告
- 国际认可的各类合规报告:
- PCI Compliance Reports

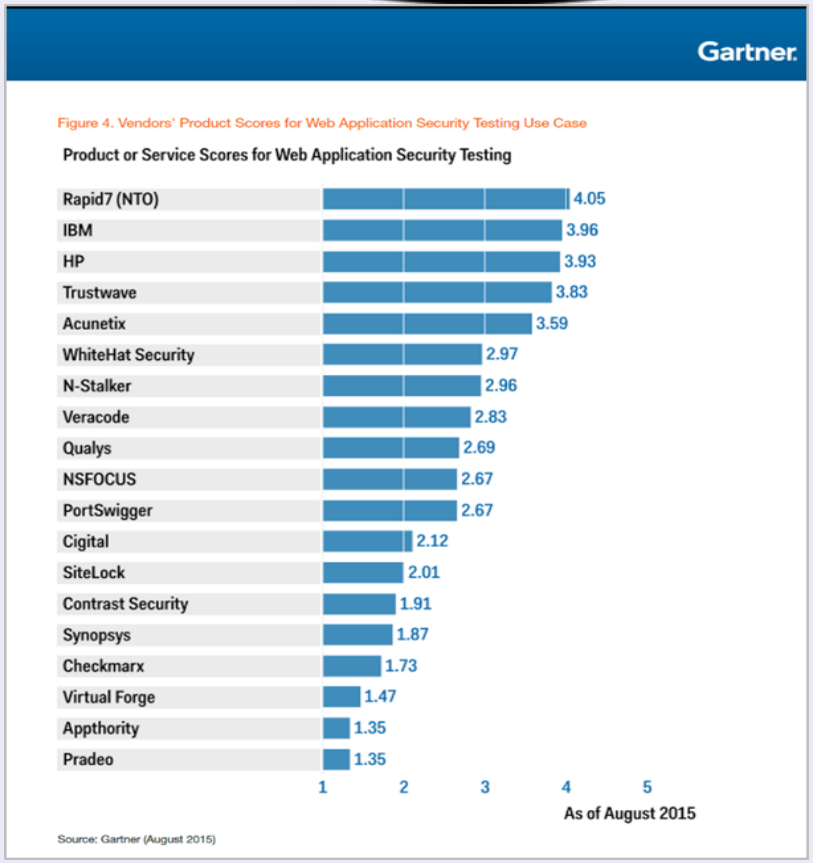
OWASP 中国
The Open Web Application Security Project

Web 风险控制
_创新的黑盒测试

Gartner 评测排名

Rapid7's offering earned the highest rating for Web AST due to DAST features. These include its **"universal translator,"** which enables testing of various types of exposed back-end interfaces, such as **JSON, REST, SOAP, XML-RPC, Google Web Toolkit (GWT) RPC and Action Message Format (AMF).** These features also include its enterprise capabilities — enterprise console, RBAC, one-click vulnerability verification, bug-tracking integration and **extensive WAF integration.**

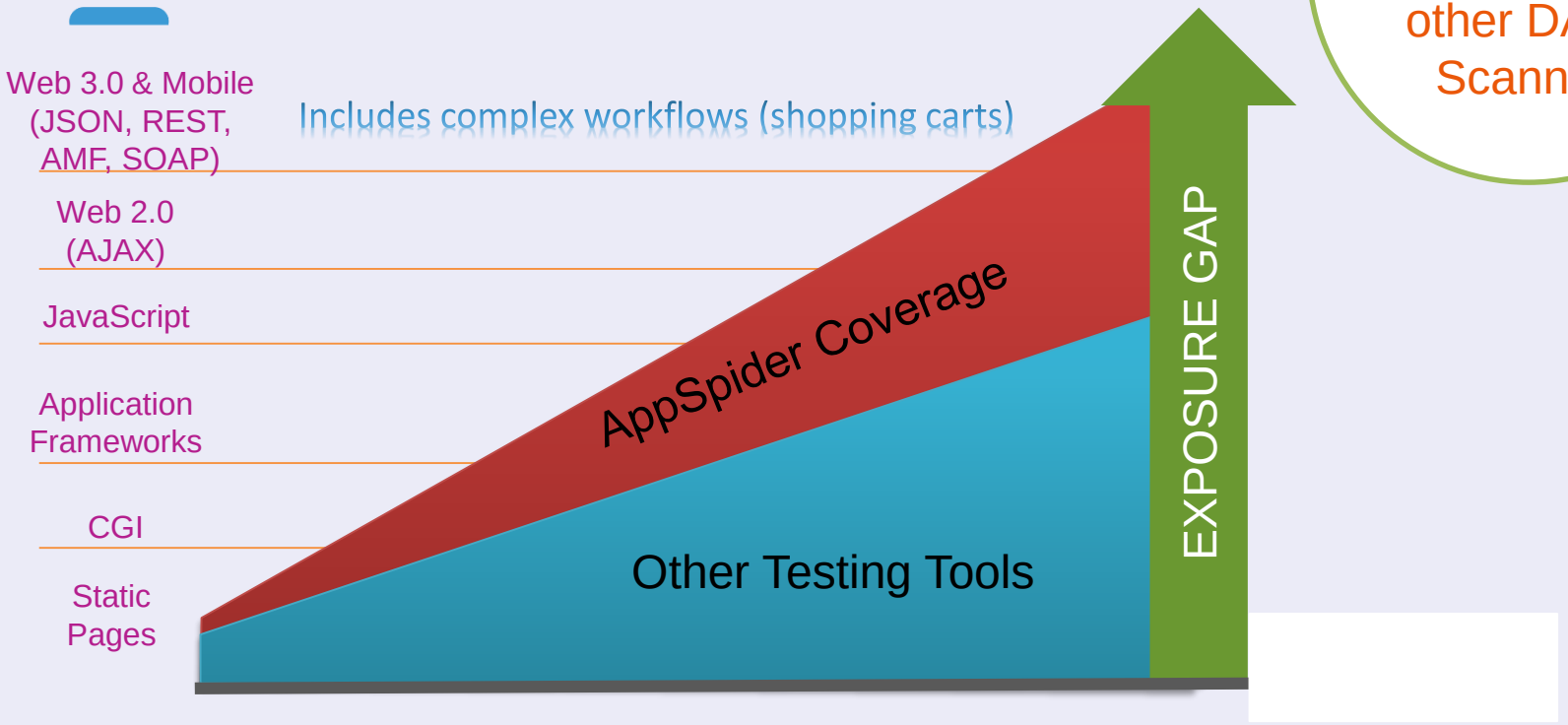
Gartner, Critical Capabilities for Application Security Testing - Joseph Feiman, Neil MacDonald, **August 17, 2015**



OWASP 中国
The Open Web Application Security Project

Universal Translator_转换器

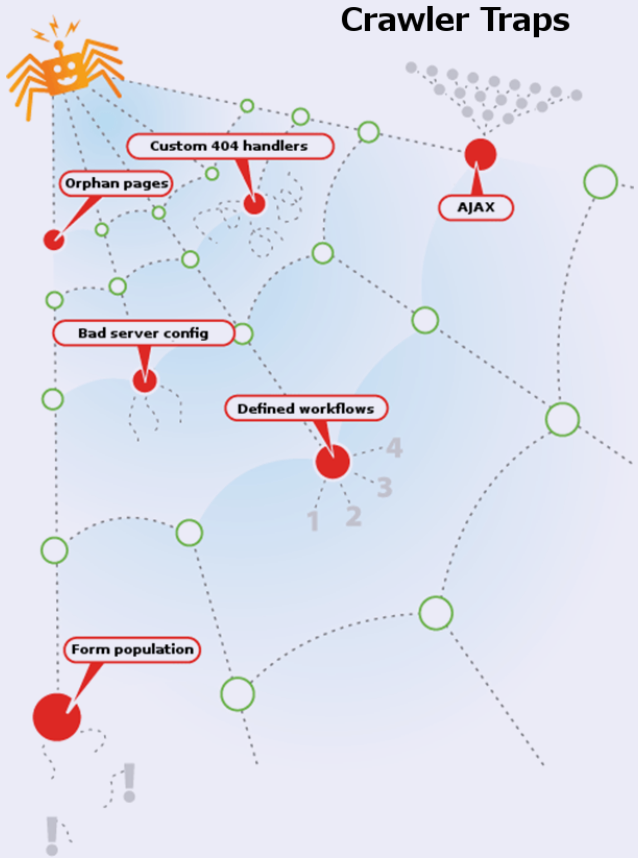
Covers more technologies than any other DAST Scanner.



扫描覆盖: 先进的网页抓取

- ***You cannot attack what you cannot crawl***

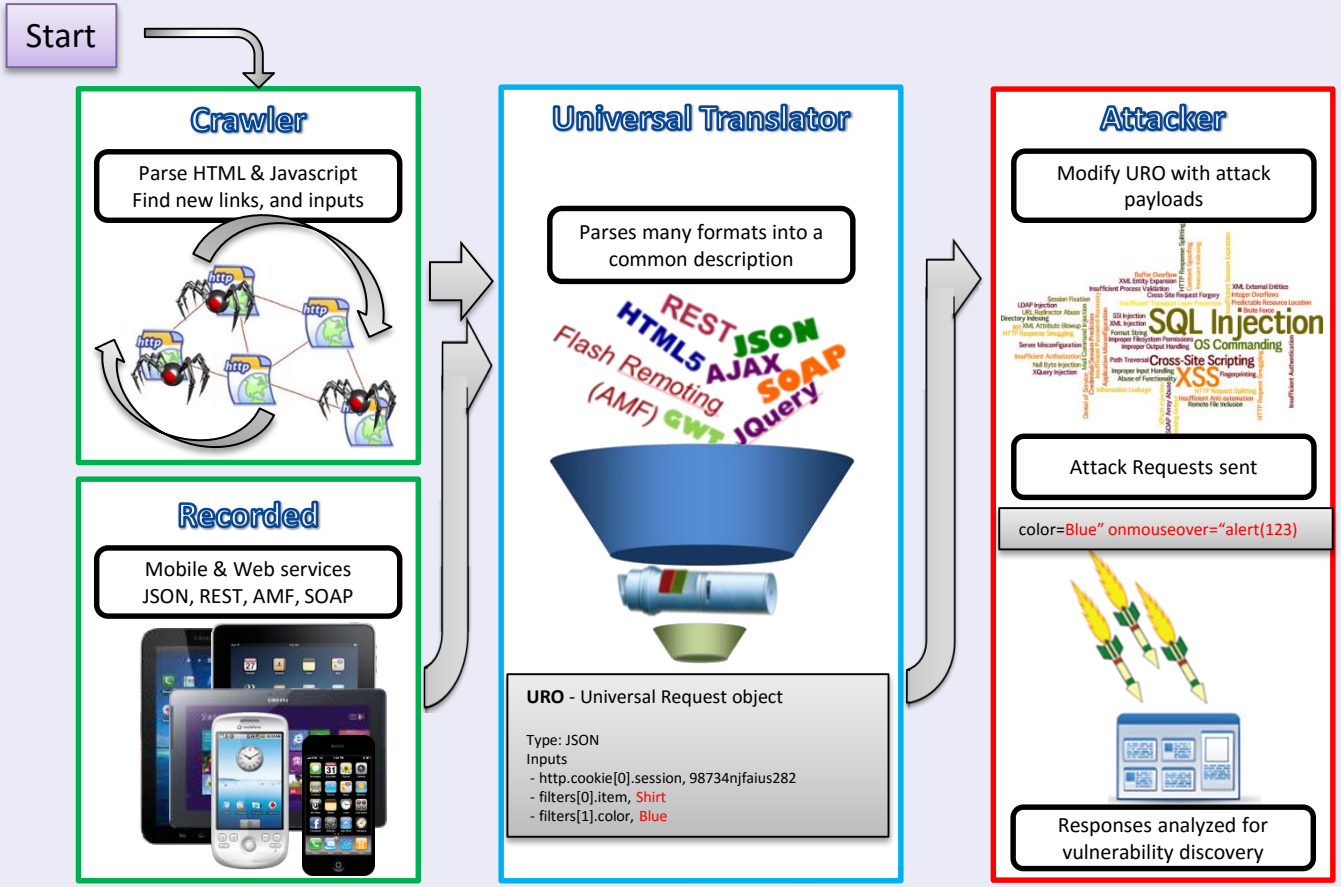
- Crucial to crawl entire site
- Limit manual training time
- Designed for human users, creates challenges for crawling
  - JavaScript & AJAX
    - Dynamic links & pages
  - Form input validation
    - Requires valid data



- 扫描需求的变化
  - 早已不是“HTML based” 的应用
  - 今天的Web应用有更多的动态内容，更加复杂

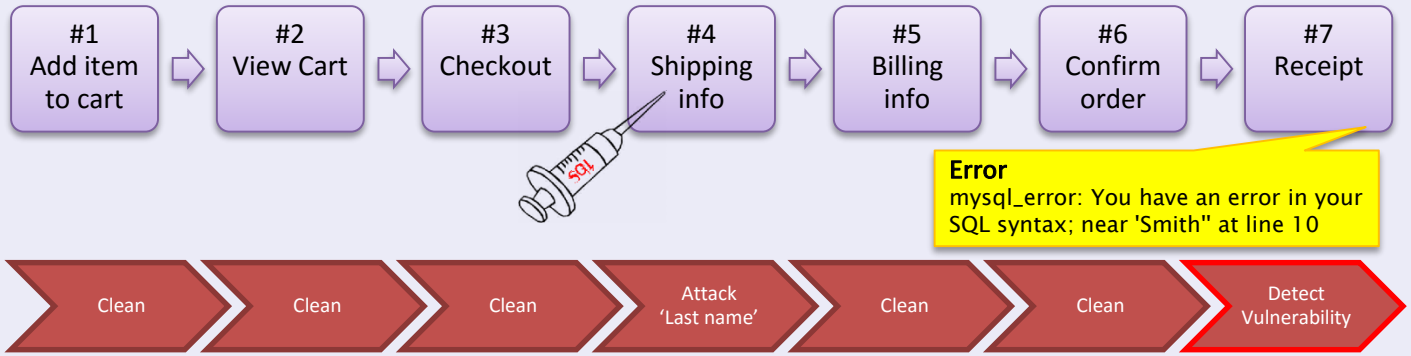
OWASP 中国
The Open Web Application Security Project

通过Universal Translator进行扫描



覆盖Web应用的流程

- **Must attack while respecting the workflow**

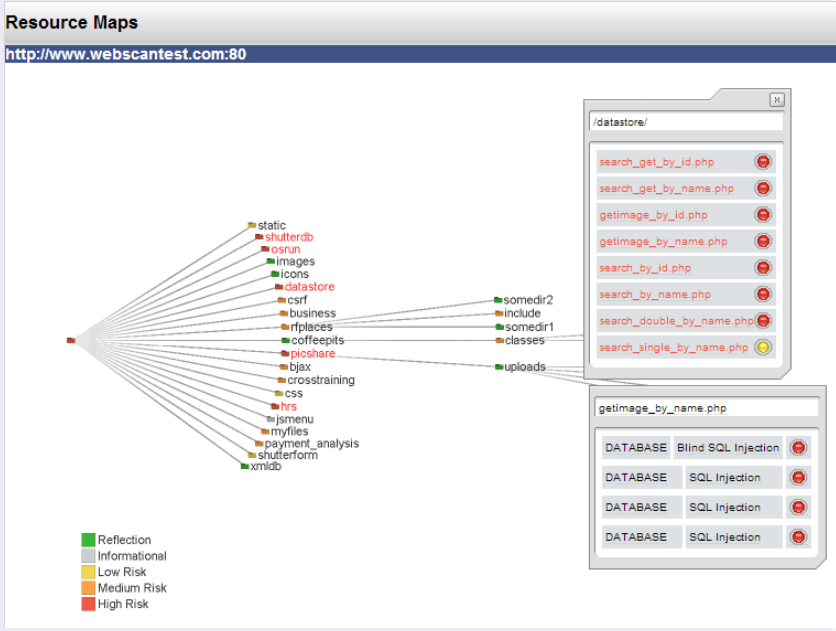


- Proper attacking must follow the expected workflow
- Only NTOSpider is able to automate this testing process

Reporting: 详细呈现抓取过程

OWASP 中国
The Open Web Application Security Project

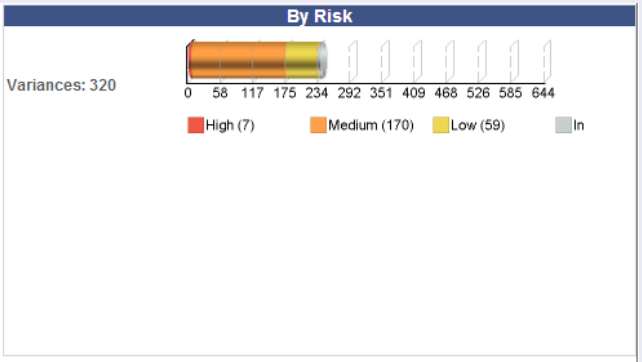
- 不能只呈现内容给审计人员
- 要给开发人员呈现更多内容
  - Enables those with better understanding of the application to assess the completeness of the scan



Reporting: 关联分析

- Consolidates numerous vulnerabilities into “Root causes”
- Facilitates prioritization, coordination and tracking of remediation

Vulnerability Type	Root Causes	Variances
Information Leakage	15	23
Reflected Cross-site scripting (XSS)	35	129
Business Logic Abuse	9	9
DOM based Cross-site scripting (XSS)	1	2
Blind SQL Injection	17	55
SQL Injection	7	28
SQL Information Leakage	7	18
HTTP Response Splitting	1	1
Credentials Over Un Encrypted Channel	2	3
Brute Force Form based Authentication	1	1
Session Fixation	2	3
SQL injection Auth Bypass	1	3
Command Injection	1	4
Buffer Overflow	6	10
Parameter Fuzzing	6	24
Unrestricted File Upload	2	7
Total:	113	320



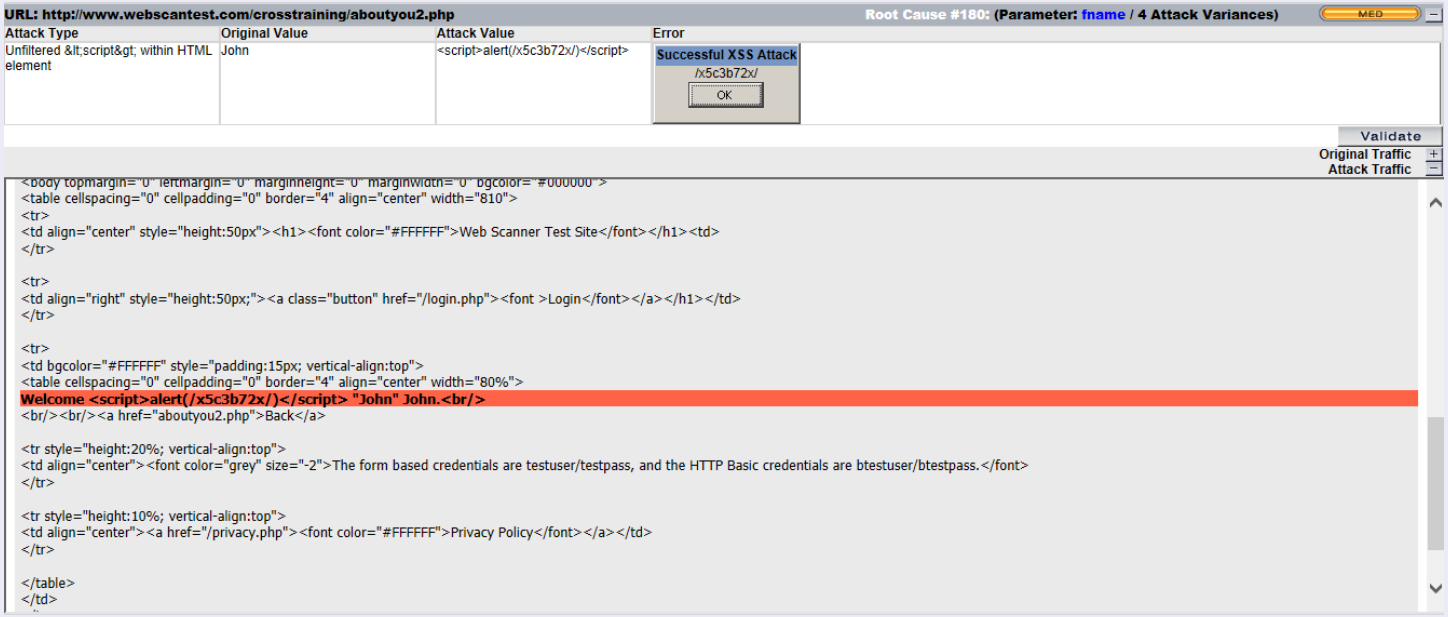
Details by Module

Disable Validate Applet
Collapse All Attacks

- Information Leakage — LOW
- Reflected Cross-site scripting (XSS) — MED
- Business Logic Abuse — LOW
- DOM based Cross-site scripting (XSS) — MED
- Blind SQL Injection — HIGH
- SQL Injection — HIGH

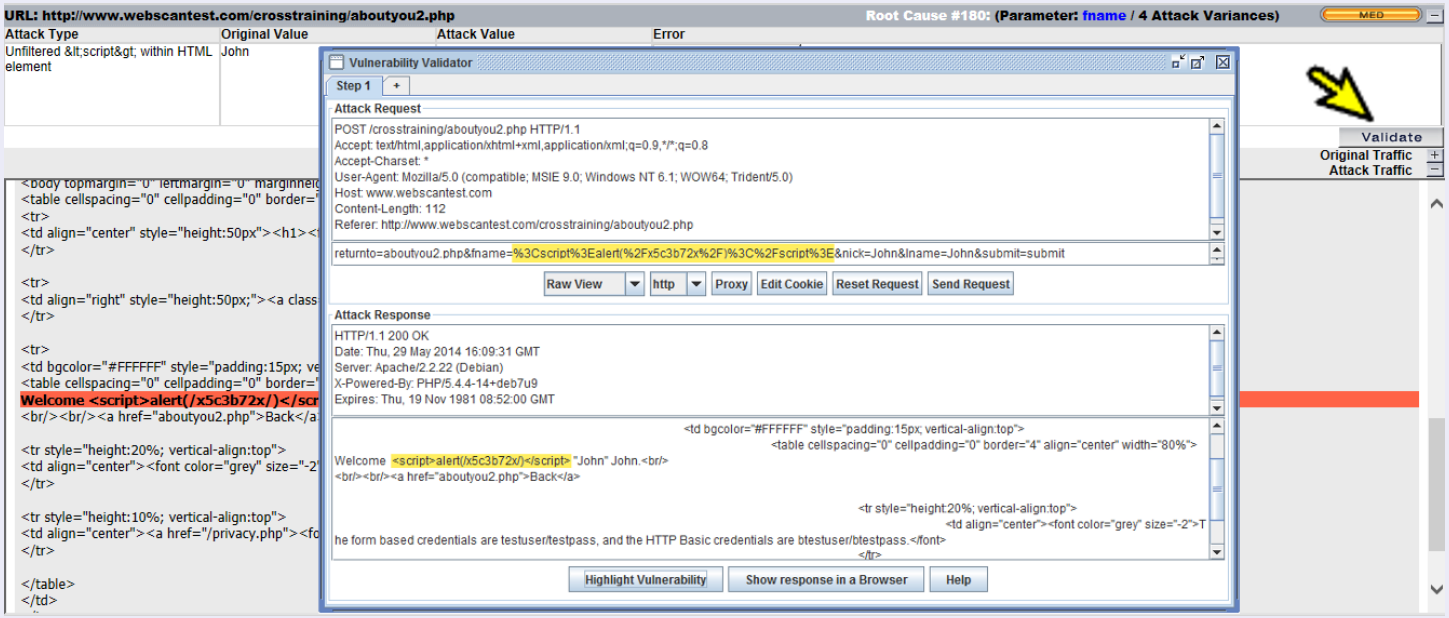
Reporting: 呈现攻击内容

- Easy to communicate source of problem to developers
- Provides simple and usable data for all levels of the process



Reporting: 呈现攻击内容

- Easy to communicate source of problem to developers
- Provides simple and usable data for all levels of the process, ***<u>including reproducing attacks</u>***



WAF / IPS联动

OWASP 中国
The Open Web Application Security Project

SOURCEfire®

- Sourcefire
- F5
- DenyAll
- Barracuda
- ModSecurity
- Imperva
- NitroSecurity

Defect Tracking联动

OWASP 中国
The Open Web Application Security Project

Jira

HP Quality Center

RSA Archer

DevOPS / SDL联动

Selenium
Jenkins
Hudson
Bamboo
Burp
Fiddler
WebScarab
Paros
Swagger
Coverity
Checkmarx

Attacks类别

OWASP 中国
The Open Web Application Security Project

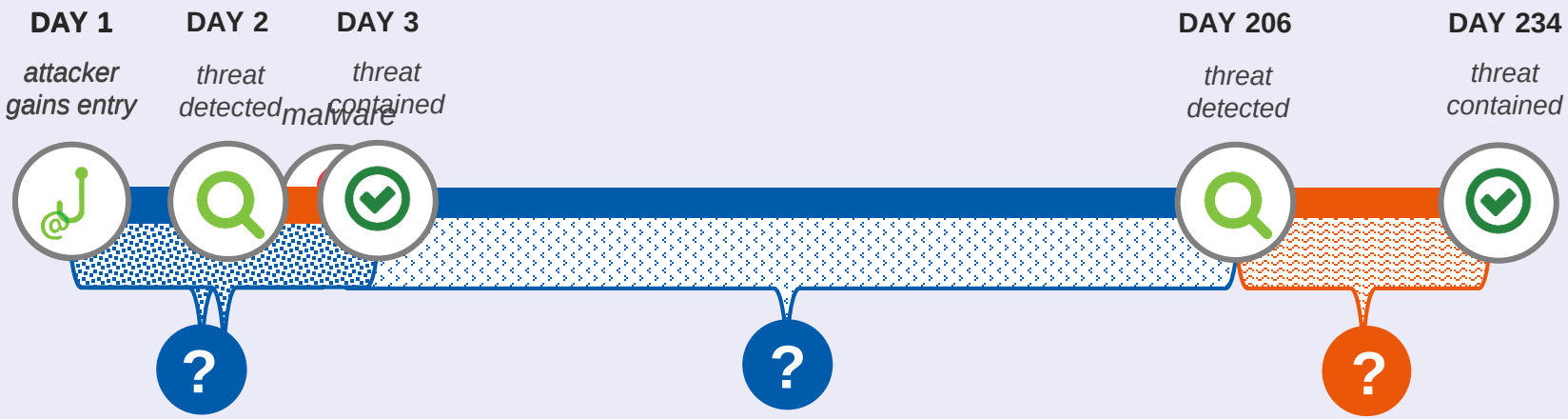
Active Attacks:
Apache Struts 2 Framework Checks
Arbitrary File Upload
ASP.Net Misconfiguration
Blind SQL Injection
Brute Force (Form Auth)
Brute Force (HTTP Auth)
Business Logic Abuse Attacks
Cross-Origin Resource Sharing (CORS)
Cross-Site Request Forgery (CSRF)
Cross Site Scripting (XSS,Reflected)
Cross Site Scripting (XSS,Simple)
Cross Site Tracing (XST)
Custom Directory Module
Custom Parameter Module
Directory Indexing
Expression Language Injection
File Inclusion
Forced Browsing
Form Session Strength
Heartbleed Check
HTTP Response Splitting
HTTPS Downgrade
Java Grinder (downloads jar files, extracts and decompiles class files and examines their content for security-related code)
LDAP Injection
OS Commanding
Parameter Fuzzing
Predictable Resource Location
Reflection Analysis
Reverse Proxy
Server Configuration
Server Side Include Injection (SSI)
Session Fixation
Session Strength
Source Code Disclosure
SQL Injection
SQL Injection Authentication Bypass
SSL Strength
Un-Validated Redirect
Web Beacon
Web Service Parameter Fuzzing
XML External Entity Attack
XPath Injection

Passive Attacks:
Apache Struts Detection
ASP.NET ViewState security
Auto Complete Attribute
Browser Cache directive (leaking sensitive information)
Browser Cache directive (web application performance)
Cookie Attributes
Credentials stored in clear test in cookies
Cross Site Scripting (DOM-Based)
E-Mail Disclosure
Information Disclosure in Comments
Information Disclosure in Response
Information Disclosure in Scripts
Information Leakage in Form Submission
Information Leakage in Responses
Privacy Disclosure
Profanity
Secure and Non-Secure Content Mix
Sensitive Data Exposure

OWASP 中国
The Open Web Application Security Project

Incident Detection and Response

尽可能缩短窗口期...

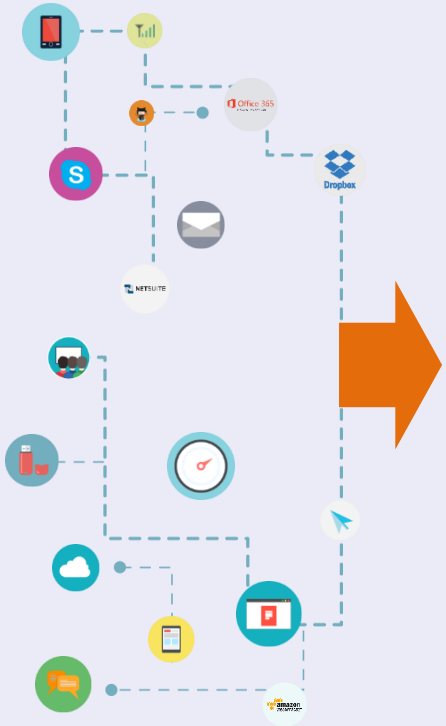


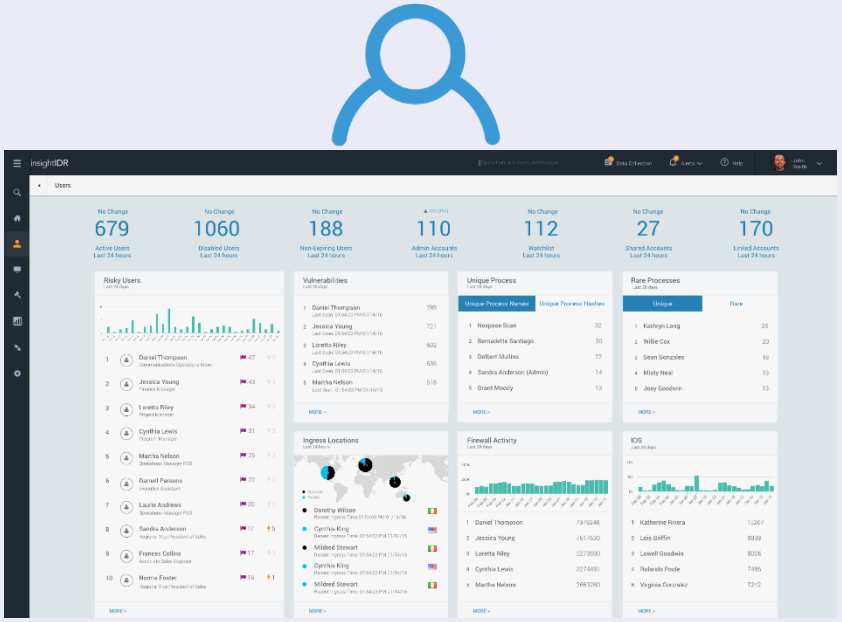
1. Detect compromise the same day
2. Scope the complete incident fast
3. Quickly hand off to remediation team

OWASP 中国
The Open Web Application Security Project

终端数据收集

- Active Directory
- LDAP
- DHCP
- DNS
- VPN
- IDS / IPS
- Web Proxy
- Firewall
- E-mail Servers
- Security Console
- Enterprise Cloud Applications
- Intruder Traps



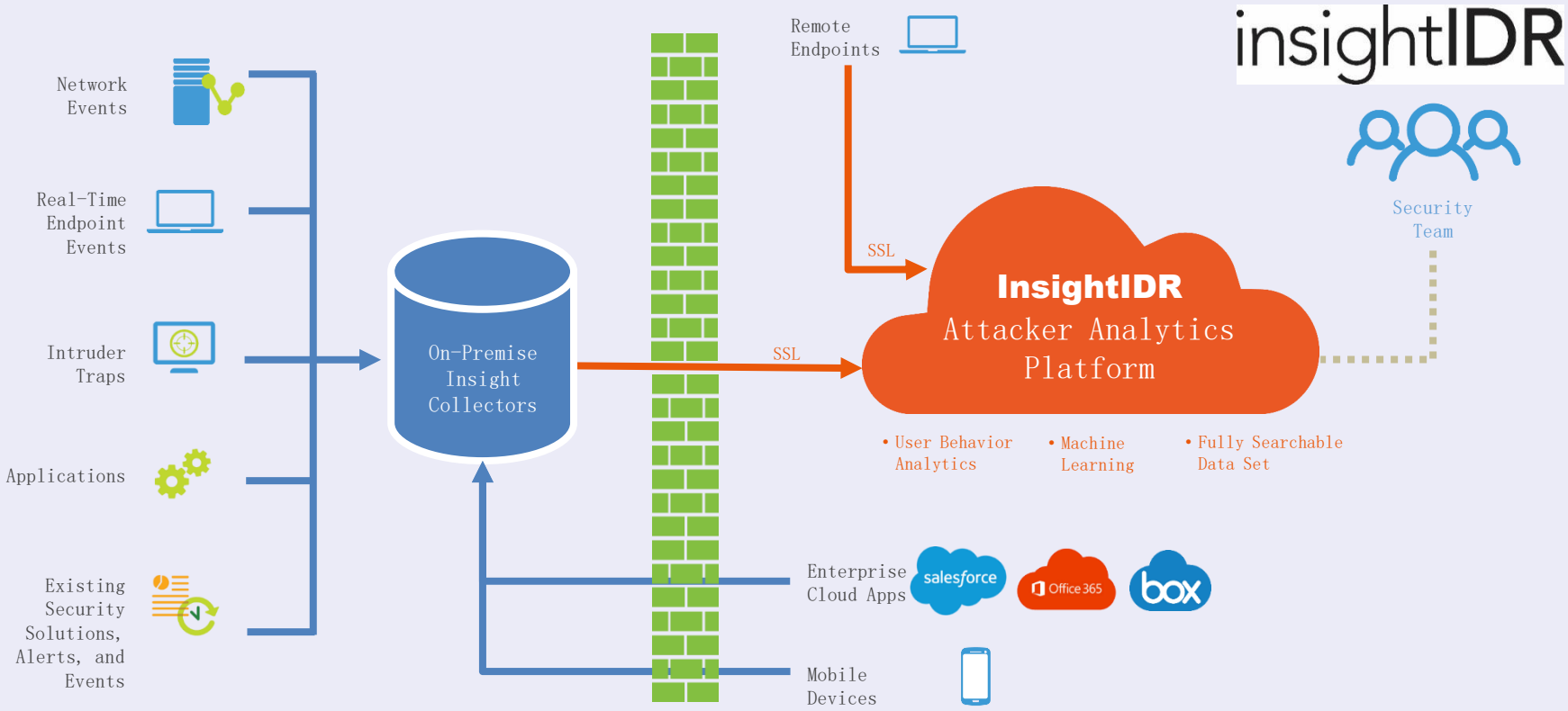


Single, Integrated Experience

RAPID7

OWASP 中国
The Open Web Application Security Project

InsightIDR Solution Architecture



RAPID7

事件源

FOUNDATIONAL EVENT SOURCES

LDAP
Microsoft Active Directory LDAP

Active Directory
Microsoft Active Directory Domain Controllers

DHCP
Cisco iOS
Infoblox Trinzic
ISC dhcpd
Microsoft DHCP

VALUE-ADD EVENT SOURCES

- DNS
- VPN
- IDS / IPS
- Web Proxy
- Firewall
- E-mail Servers
- Security Console
- Enterprise Cloud Applications
- Intruder Traps

OWASP 中国
The Open Web Application Security Project

DNS
ISC Bind9
Infoblox Trinzic
Microsoft DNS
MikroTik
PowerDNS

Data Exporters
FireEye Threat Analytics Platform
HP ArcSight & ArcSight Logger
Splunk

VPN
Cisco ASA VPN
F5 Networks FirePass
Fortinet FortiGate
Juniper SA
Microsoft IAS (RADIUS)
Microsoft Network Policy Server
Microsoft Remote Web Access
OpenVPN
SonicWALL Firewall & VPN

Web Proxy
Barracuda Web Filter
Blue Coat Proxy
Cisco IronPort
Fortinet FortiGate
Intel Security (fka McAfee) Web Reporter
Sophos Secure Web Gateway
Squid
Watchguard XTM
WebSense Web Security Gateway

E-mail
Microsoft ActiveSync (mobile devices)
Microsoft Exchange
Outlook Web Access

Firewall
Check Point Firewall
Cisco ASA Firewall & VPN
Cisco Meraki
Fortinet Fortigate
Juniper Netscreen
Palo Alto Networks Firewall
SonicWALL
Sophos Firewall
Stonesoft Firewall
Watchguard XTM

IDS / IPS
Cisco Sourcefire
Dell iSensor
Dell SonicWall
HP TippingPoint
McAfee IDS
Metaflows IDS
Security Onion
Snort

Rapid7
Windows Agentless Endpoint Monitor
Mac Agentless Endpoint Monitor
Honeypot & Honey Users
Metasploit
Nexpose
Sophos Enduser Protection
Symantec Endpoint Protection

Cloud Services
AWS Cloud Trails
Box.com
Duo Security
Google Apps
Office 365
Okta
Salesforce.com

Advanced Malware
FireEye NX
Palo Alto Networks WildFire

SIEMs/Log Aggregators
HP ArcSight
IBM QRadar
Intel Security (fka McAfee) NitroSecurity
LogRhythm
Splunk

Virus Scanners
McAfee ePO
Sophos Enduser Protection
Symantec Enduser Protection

Application Monitoring
Atlassian Confluence
Microsoft SQL Server

RAPID7

攻击链条

Infiltration and Persistence
- Phish users
- Use leaked credentials
- Connect to network
- Anonymize access
- Deploy backdoors

Reconnaissance
- Get user list
- Scout targets
- Find vulnerabilities

Lateral Movement
- Access machines with credentials
- Collect more passwords
- Increase privileges

Mission Target
- Access critical data
- Upload data to external location

Maintain Presence
- Deploy backdoors
- Continued check-ins for future use

OWASP 中国
The Open Web Application Security Project

insightIDR

有效打断攻击链条

Infiltration and Persistence

- Detect phishing attempts
- Identify malware
- Alert on leaked credentials
- Monitor inbound connections

Reconnaissance

- Detect network scans

Lateral Movement

- Detect intruders switching identities
- Detect unusual authentications
- Identify malware
- Identify privilege escalation
- Detect password guessing attempts & pass-the-hash

Mission Target

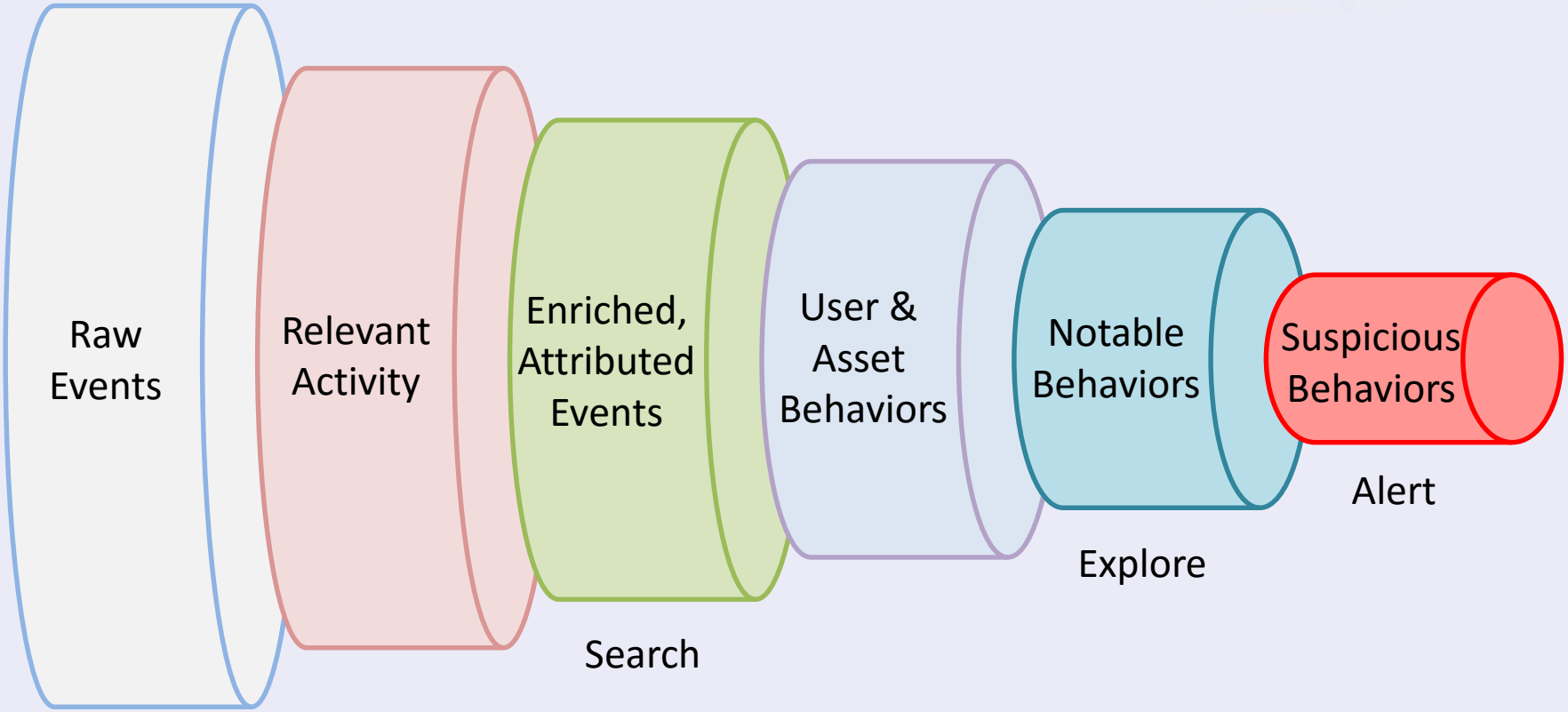
- Detect suspicious access to critical data
- Monitor data traffic and cloud usage

Maintain Presence

- Detect malicious processes

RAPID7

信息筛选


Raw Events
Relevant Activity
Enriched, Attributed Events
User & Asset Behaviors
Notable Behaviors
Suspicious Behaviors
Search
Explore
Alert

Search - It's All About The Context

- Would you like to search through *this*?

  09 2016 21:10:54 R7-BOS-5545 : %ASA-6-302014: Teardown TCP connection 406359796 for outside:52.2.119.185/443 to INSIDE:10.1.86.49/57672 duration 0:00:14 bytes 4510 TCP FINs

- Or **THIS?**

{ "timestamp": "2016-03-09T21:10:54.000Z",
"asset": "kx240-2543.acme.com",
"user": "Ronald Serpico",
"source_address": "52.2.119.185",
"source_port": "443",
"destination_address": "10.1.86.49",
"destination_port": "57672",
"direction": "INBOUND",
"incoming_bytes": "4510",
"outgoing_bytes": "0",
"geoip_organization": "Amazon.com",
"geoip_country_code": "US",
"geoip_country_name": "United States",
"geoip_city": "Ashburn",
"geoip_region": "VA" }

更好的解决方案交付

OWASP 中国
The Open Web Application Security Project

Executive Summary of Findings

Cyber Security Maturity Rating Methodology

Strategic Recommendations

Cyber Security Maturity Assessment Score Card

Acme Company Maturity

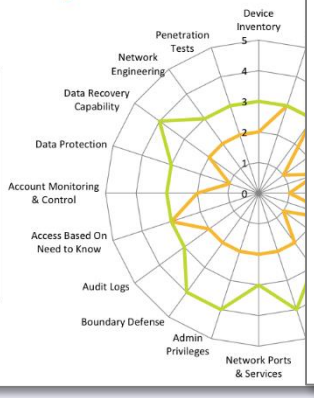
Tactical Recommendations

Cyber Security Maturity Assessment Sc

Acme Company

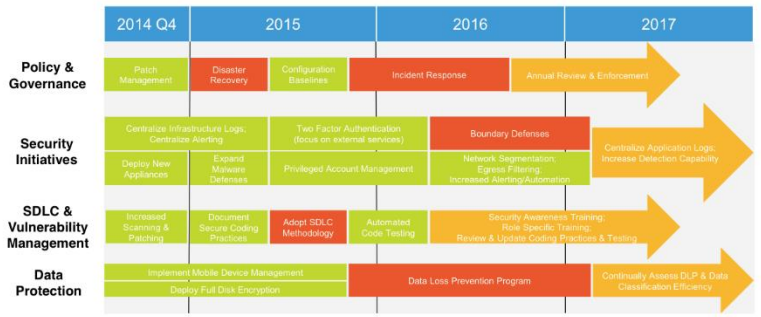
Current State: 2.00
Managed (Level 2)

Target State: 3.25
Standardized (Level 3)



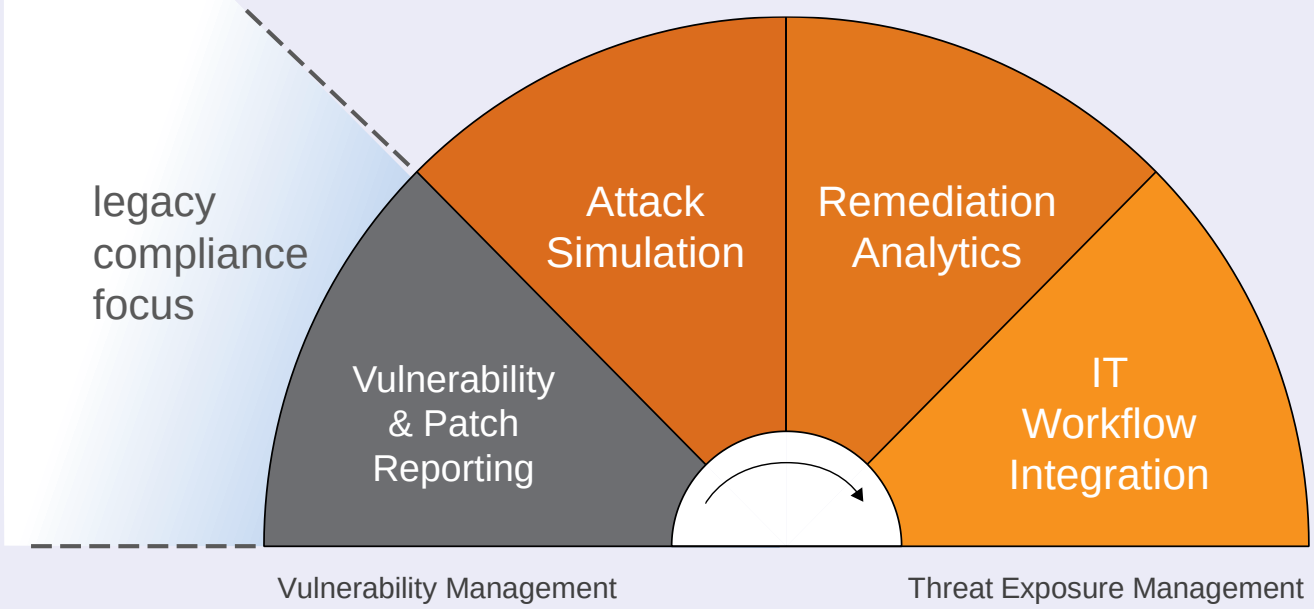
Acme Security Roadmap

Key: Tactical Strategic Ongoing



RAPID7

Confidential and Proprietary 13

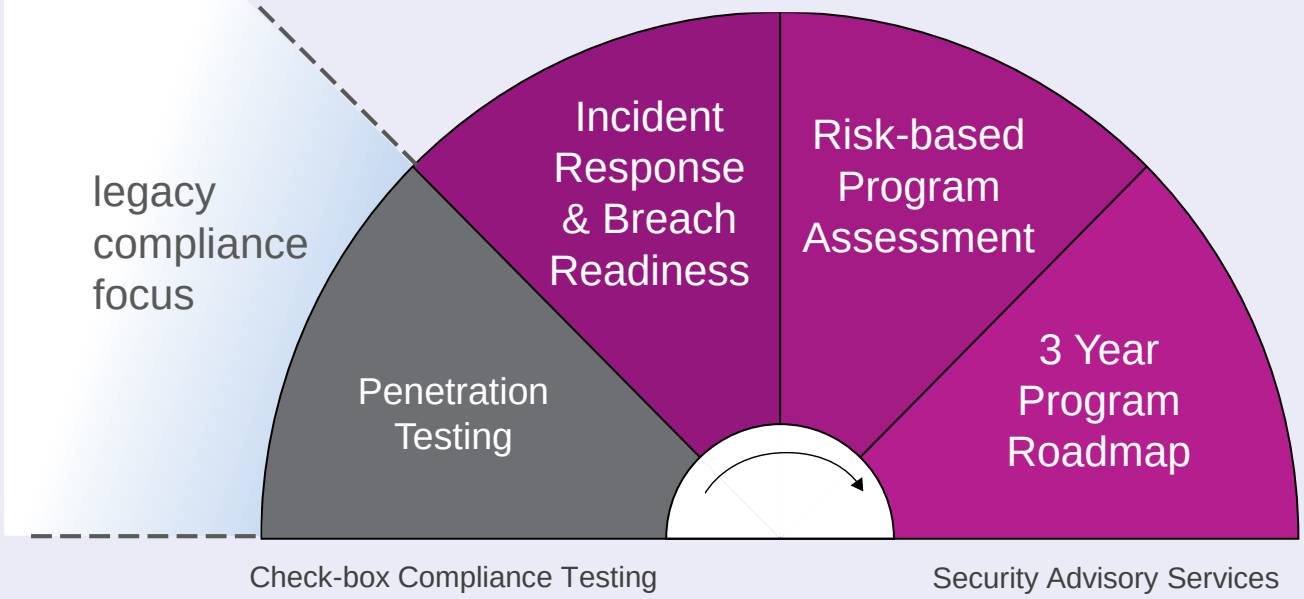


Rapid7 Threat Exposure Management:

- ✓ *Know your weak points*
- ✓ *Prioritize what matters*
- ✓ *Optimize remediation*

RAPID7 TECHNOLOGY:

nexpose® vulnerability management | metasploit® attack simulation | appspider web application assessment



Rapid7 Security Advisory Services:

- ✓ *Quantify Security Status*
- ✓ *Gain Executive Alignment*
- ✓ *Make Measurable Progress*

RAPID7 TECHNOLOGY:	Security Assessment	Program Development

OWASP 中国
The Open Web Application Security Project

RAPID7

NASDAQ: RPD

Delivering Security Data & Analytics

that revolutionize the practice of cyber security

5,100+	37%	99	800+
Customers	Fortune 1000	Countries	Employees