

ACI – Third-Party Software Vulnerability Tracking Process

Who is ACI?

ACI is a software product and services company

- In business since 1975
- 30+ products mostly dealing with financial transactions
- 2000+ employees worldwide
- 800+ customers in 88 countries
- Last year – 80 billion consumer payment transactions
- Estimate $5 trillion in wholesale payments per day

Why Track Third-Party vulnerabilities?

PCI Requirement

- PCI-DSS v1.1 section 6.2
- PABP v1.4 section 7.1

Risk Management

- Customers may not test third-party patches
  - Don't want system outage
  - Attackers exploit these vulnerabilities in hopes that system updating is slow.
- Proactive position with regards to notification

Good Business

Third-Party Software

Operating Systems
- Guardian, HP-UX , AIX, OS/390, z/OS, Windows

Middleware
- Databases
  - C-Tree, Enscribe, VSAM, SQL Server, Oracle, DB2
- Messaging
  - WebSphereMQ
- Web Application Server
  - Tomcat, WebSphere, WebLogic
- HTTP Server
  - Apache, IIS

Java SDKs, JVMs

Libraries, including open-source

Third-Party Vulnerability Tracking Participants

Security Engineering

- Overall support of system
- First level filtering for false positives

Product Lead

- Document dependency on third-party products
- Second level filtering for false positives
- Testing of third party patches with current release
- Forward issues to Product Development
- Inform Customer Management of status

Product Development

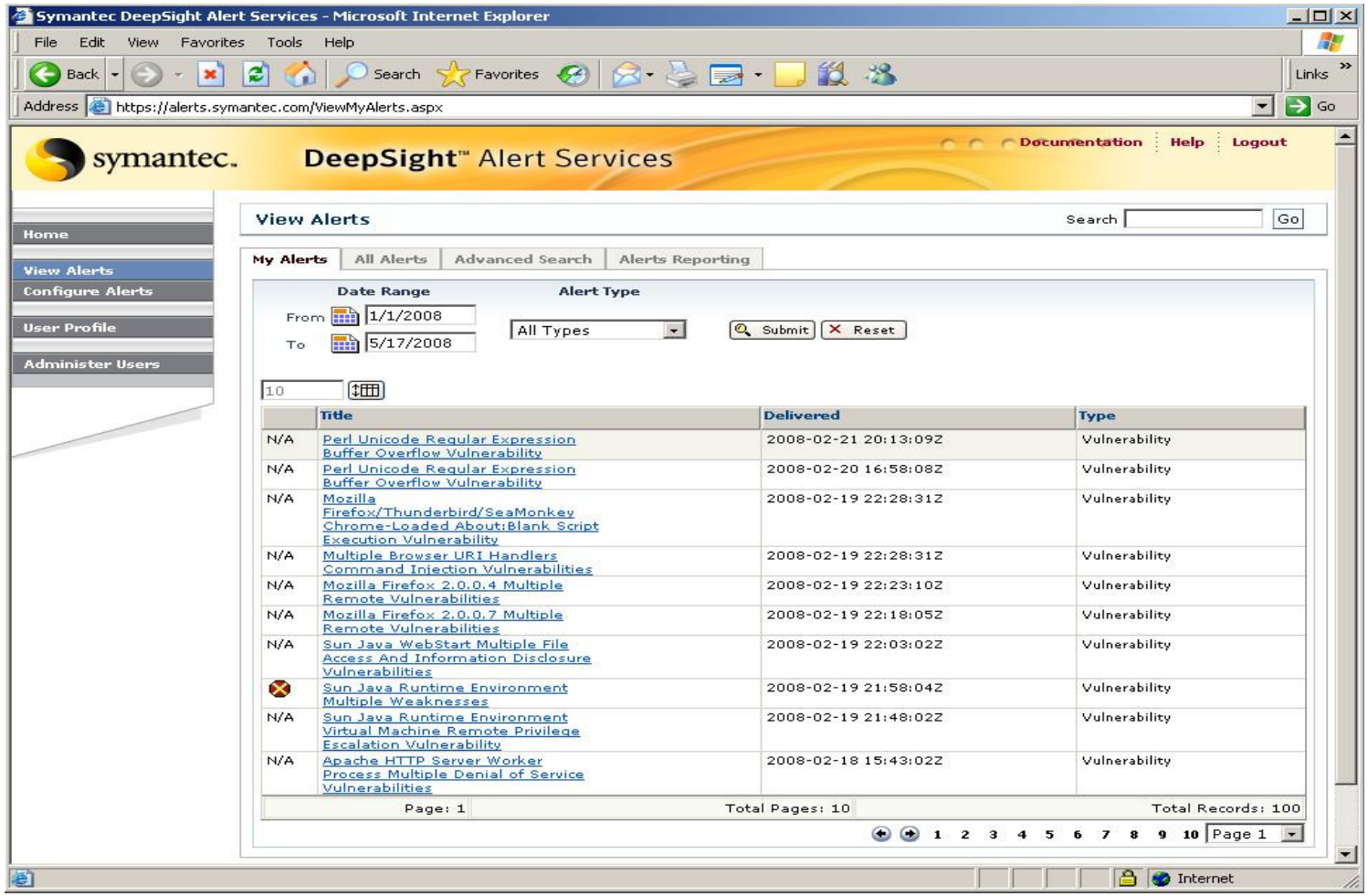
- Provide product fixes
- Notify Product Lead when complete

Customer Management

- Notify Customers of vulnerabilities and fixes

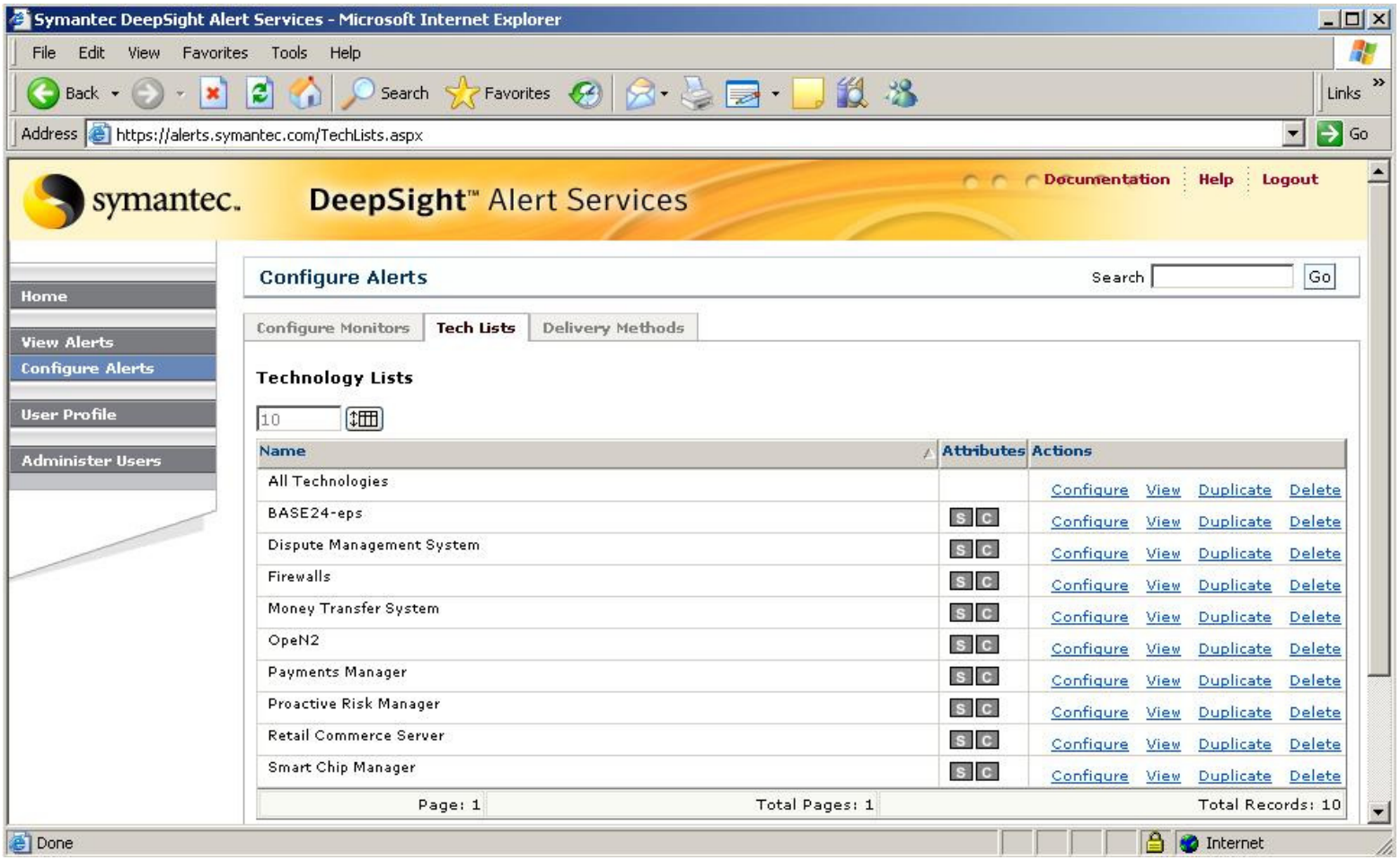
Third-Party Tracking Process

ACI Subscribes to Symantec DeepSight Alert Service



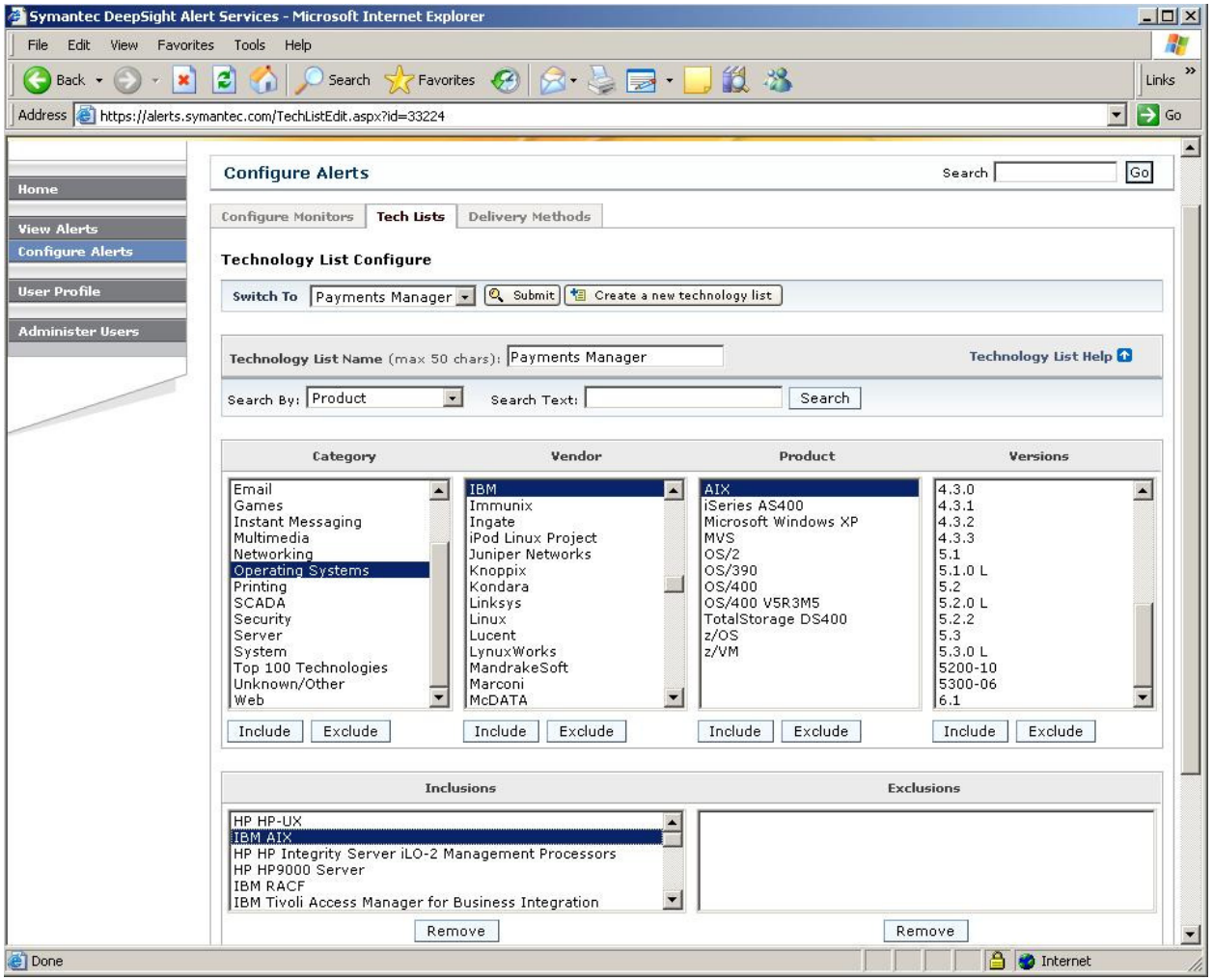
DeepSight Configuration

A new “Technology” is added for each ACI product



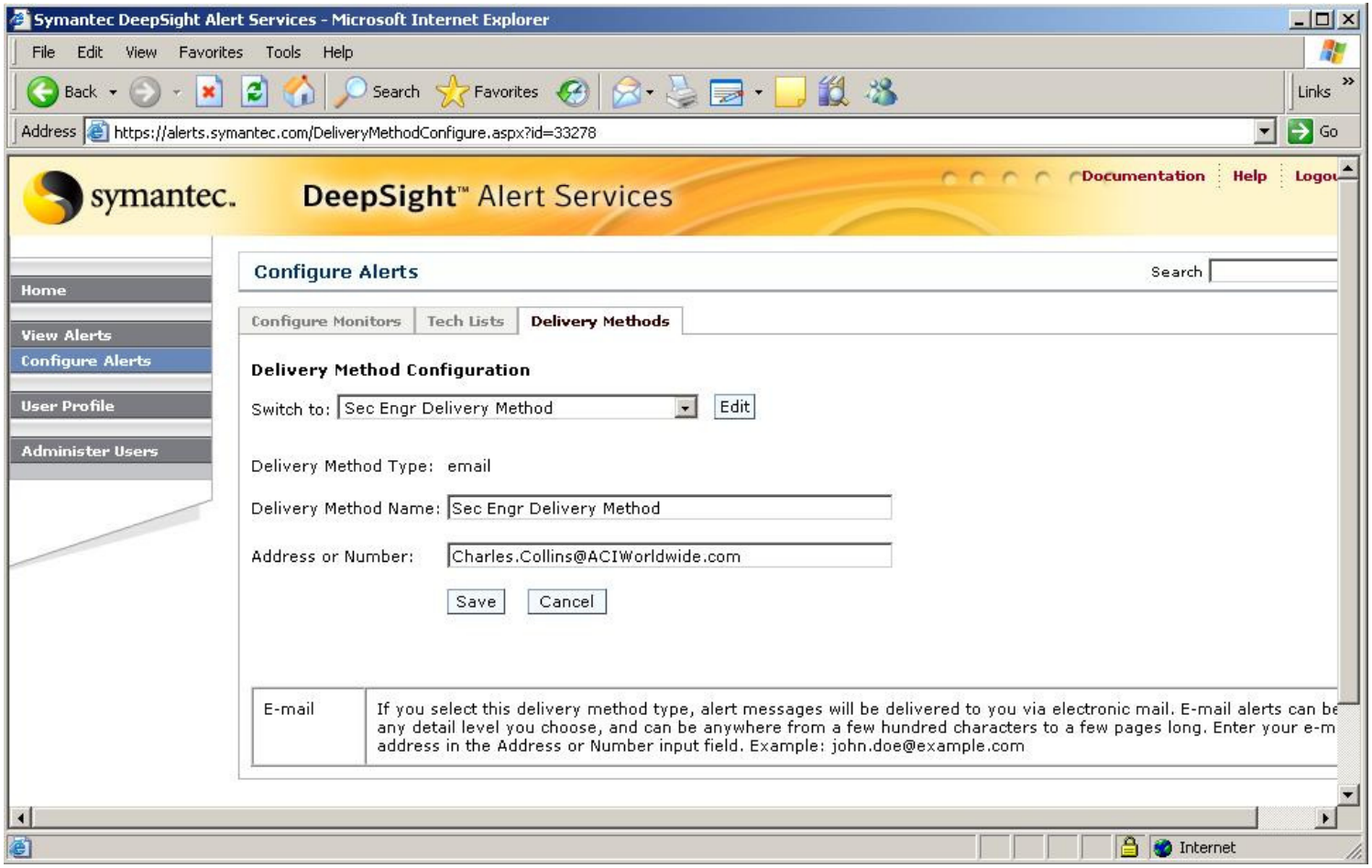
DeepSight Configuration (cont.)

Third-Party Software is monitored for each “Technology”.

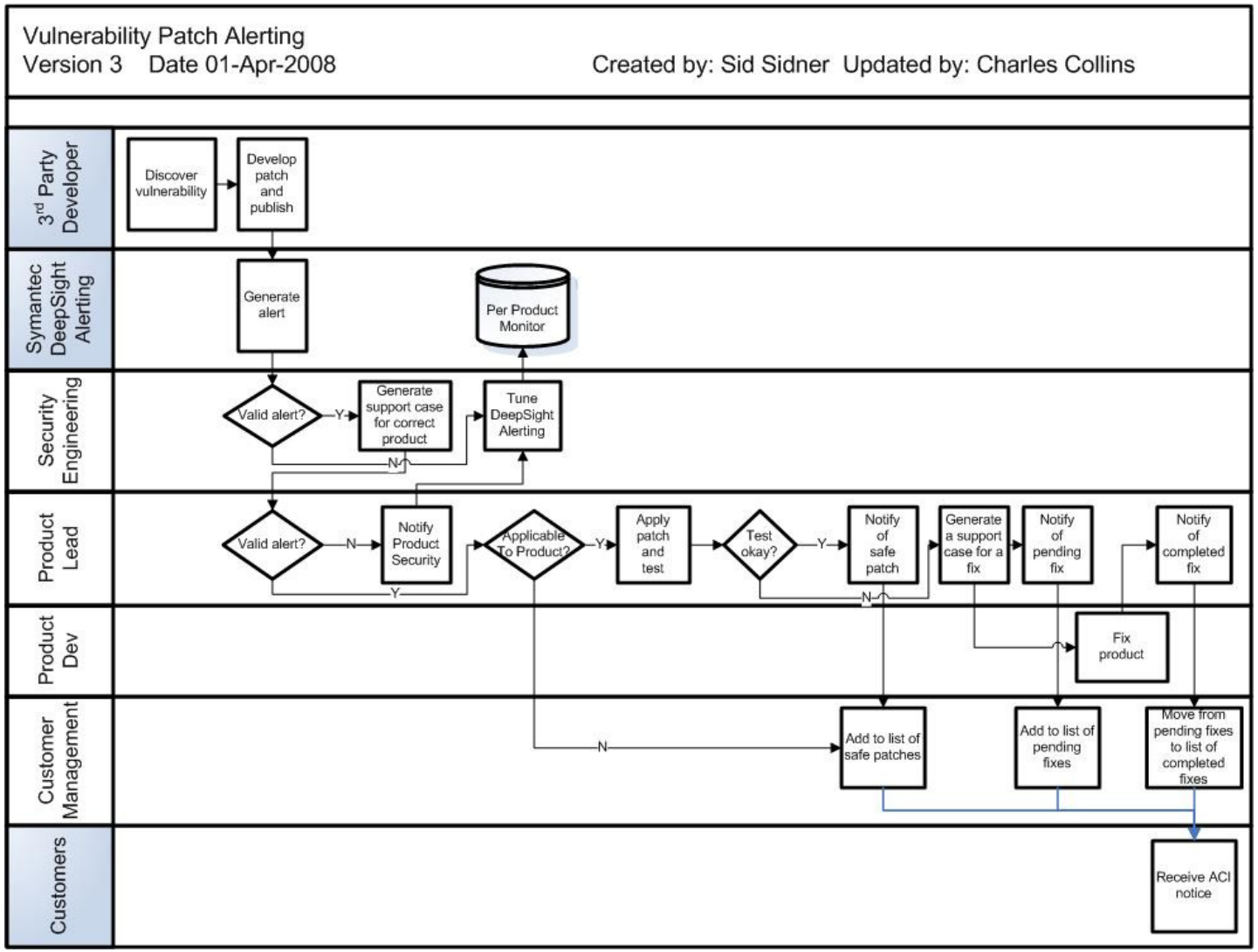


DeepSight Configuration (cont.)

Email Alerts are Forwarded for Each Reported Vulnerability



Vulnerability Tracking Process Flow




EVERY SECOND. EVERY DAY.