Automating Vulnerability Management in a Heterogeneous Enterprise

Jeff Boerio
Sr. Information Security Specialist
Information Security Management

June, 2008

Legal Notices

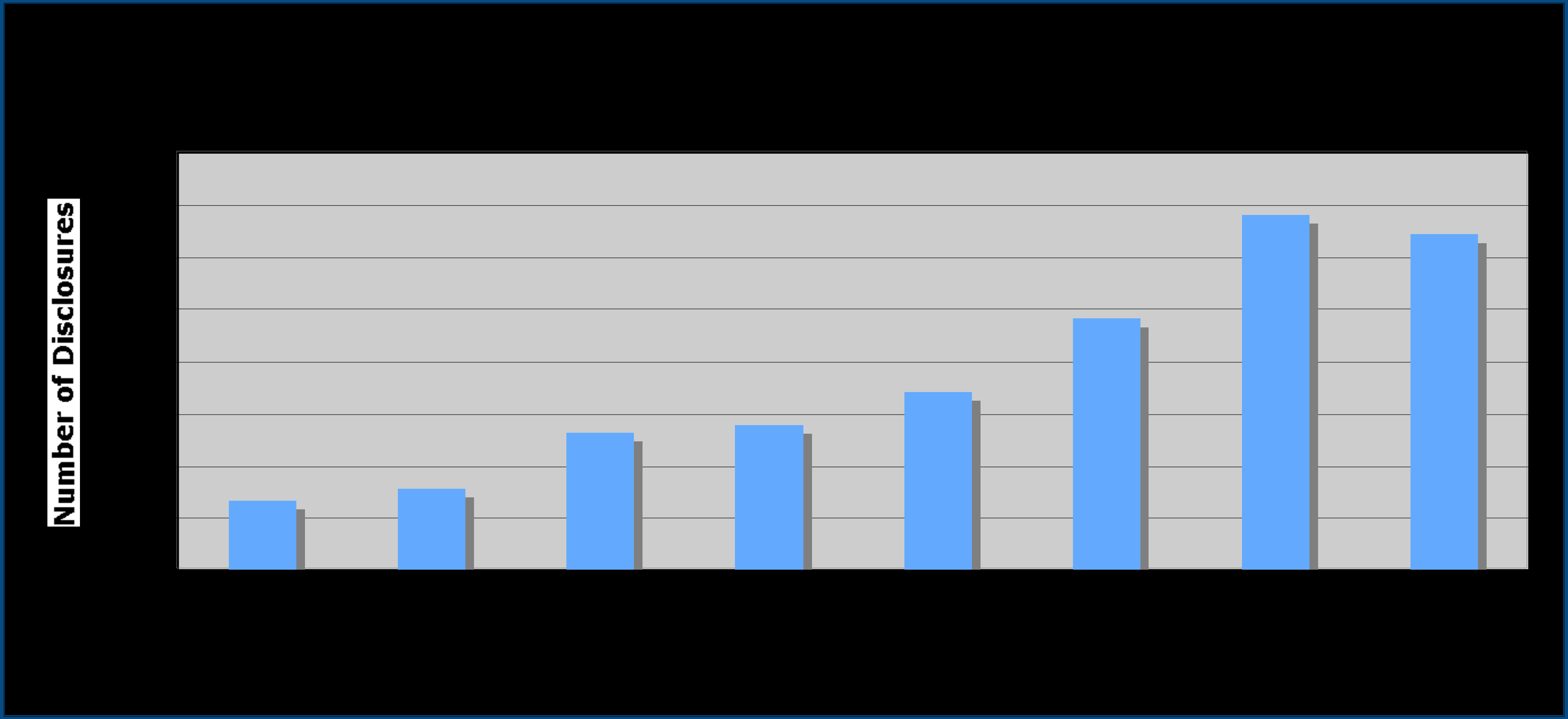
This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Last Updated: Aug 28, 2006

Introduction

- Background on vulnerability run rates
- Drivers for automation
- Discuss the vulnerability alert process
- Framework for automating the alert process
- Q & A

Vulnerability Run Rate *



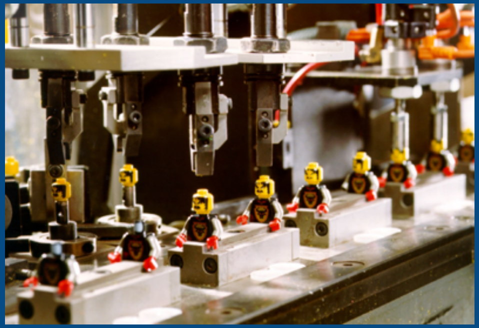
* X-Force: http://www.iss.net/documents/literature/x-force_2007_trend_statistics_report.pdf

Drivers for Automation

- Volume

- Speed

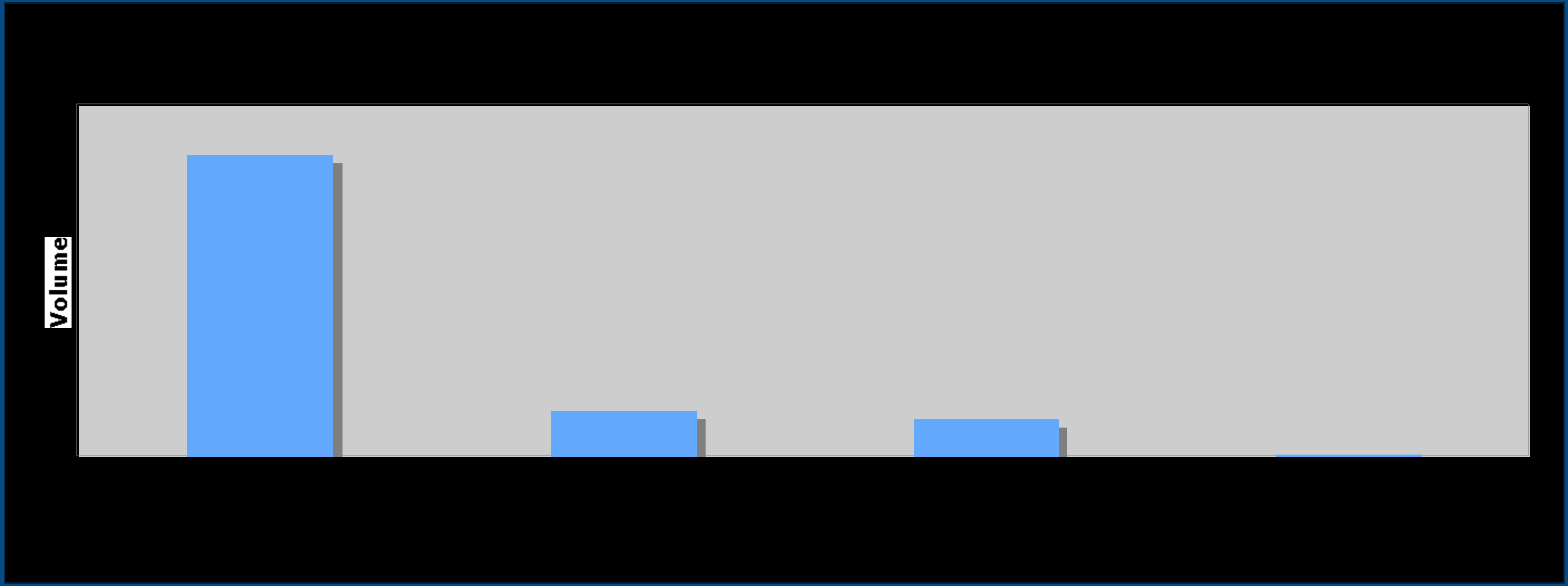
- Accuracy, Consistency



- Cost

Guillotine Lego from mrcaro.blogspot.com

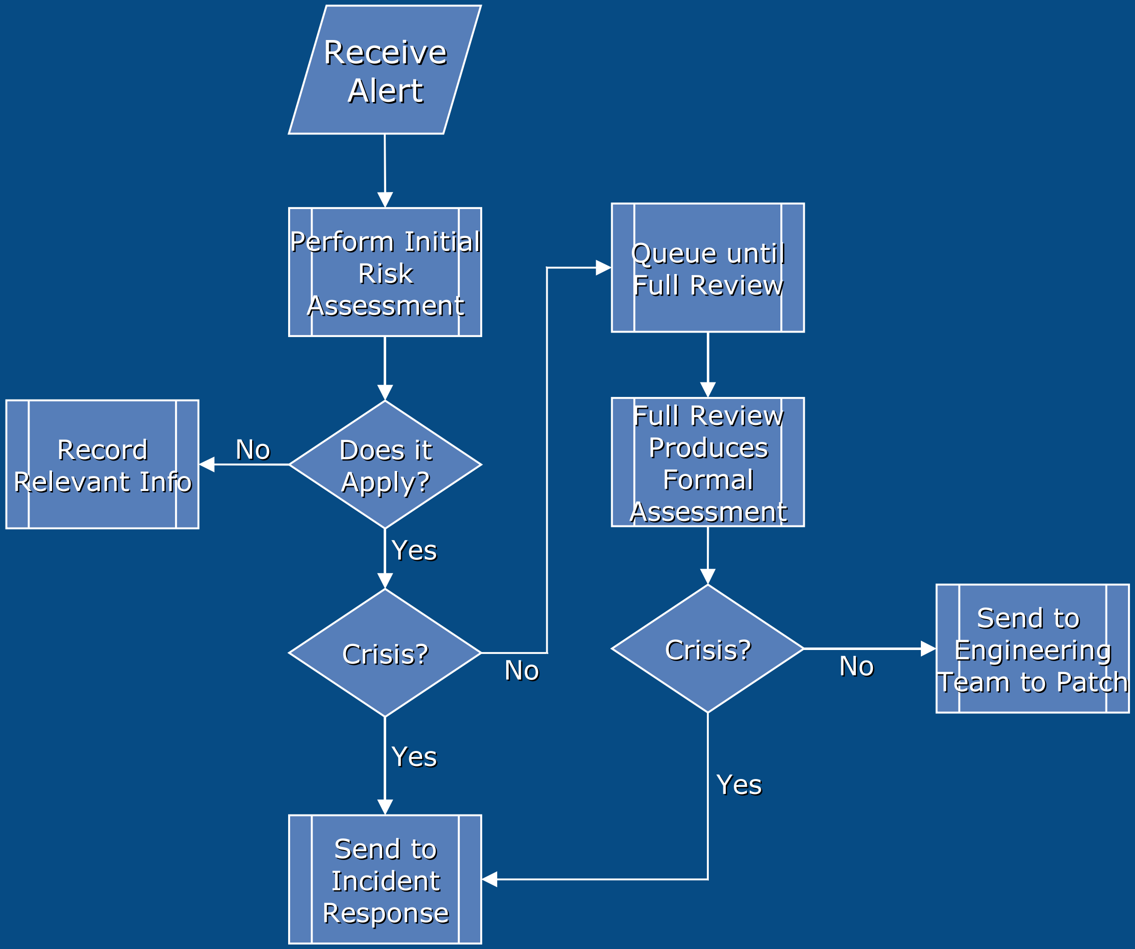
Alert Volume



Significant majority of vulnerability reports do not apply to us.

We spend almost as much time reviewing those reports as we do for vulnerabilities that do apply.

Alert Process



Receive Alert
Perform Initial Risk Assessment
Does it Apply?
No
Record Relevant Info
Yes
Crisis?
No
Queue until Full Review
Full Review Produces Formal Assessment
Crisis?
No
Send to Engineering Team to Patch
Yes
Yes
Send to Incident Response

Pseudocode 101

- Object Alert
  - Vendor
  - Product
  - Severity
  - Initial Rating
- Function isUsed()
- Function lookupSeverity()
- Procedure dbRecord()
- Procedure processAlert()

Automation 101

```
new Alert;
if isUsed(Alert->Product) {
     if (Alert->Severity >= HIGH_THRESHOLD) {
           dbRecord(Alert->InitialRating, HIGH);
           processAlert(Alert, HIGH);
     } else if (Alert->Severity >= MODERATE_THRESHOLD) {
           dbRecord(Alert->InitialRating, MODERATE);
           processAlert(Alert, MODERATE);
     } else {
           dbRecord(Alert->InitialRating, LOW);
           processAlert(Alert, LOW);
     }
} else {
     dbRecord(Alert->InitialRating, NA);
     processAlert(Alert, NA);
}
```

Automation 201

```
new Alert;
if  isUsed(Alert->Product) {
     if (Alert->Severity >= lookupSeverity(Alert->Vendor, HIGH) {
            dbRecord(Alert->InitialRating, HIGH);
            processAlert(Alert, HIGH);
     } else if (Alert->Severity >= lookupSeverity(Alert->Vendor,MODERATE) {
            dbRecord(Alert->InitialRating, MODERATE);
            processAlert(Alert, MODERATE);
     } else {
            dbRecord(Alert->InitialRating, LOW);
            processAlert(Alert, LOW);
     }
} else {
     dbRecord(Alert->InitialRating, NA);
            dbRecord(Alert->InitialRating, NA);
            procesAlert(Alert, NA);
}
```

Extra Credit: If your alert service/process offers updates, this process can be extended to cover that capability

Report Card

The automation of vulnerability assessment:

- Puts alert info in hands of engineers quicker
- Reduces number of assessment “re-rates”
- Results in less time spent reviewing data
- Implementation cost was negligible

Questions

Jeff Boerio
jeff.boerio@intel.com

Intel Corporation
23215 NE Evergreen Parkway
M/S EG1-105
Hillsboro, OR 97124

intel®

Leap ahead™