xtract

xla Threat Reduction, Analysis & Correlation Tool.

Introduction

1. Automation needed to handle EINSTEIN (E^3A) notices:
   - How can we handle large volumes of notices?
   - Can we prioritized the data?
   - Can we derive information from the data?
   - Does the aggregate of this information mean something?
2. Benefits realized:
   - Cost savings
   - Improved efficiency
3. Continuous Monitoring Strategy:
   - Security Manager
   - Risk Analyst
   - Security Analyst
4. Securely developed application

xtract ***technology was developed by XLA to meet the needs of an existing EINSTEIN3 customer and continues to be used today.***

xTRACT Automated Process

We **MIGHT** have a problem…?

We **HAVE** a problem!

Our problem is **RIGHT HERE !!**

xtract

Data

Notices received from EINSTEIN

E³A Notice

- **Timestamp**
- ~~Reference #~~
- ~~Destination~~
- ~~Source (firewall)~~

Information

Single or multiple notices grouped together

xTRACT Event

- **Time span**
- **Reference #**
- **Network Activity**
- **User**
- **Source IP Address**
- **URL**
- **more**

Knowledge

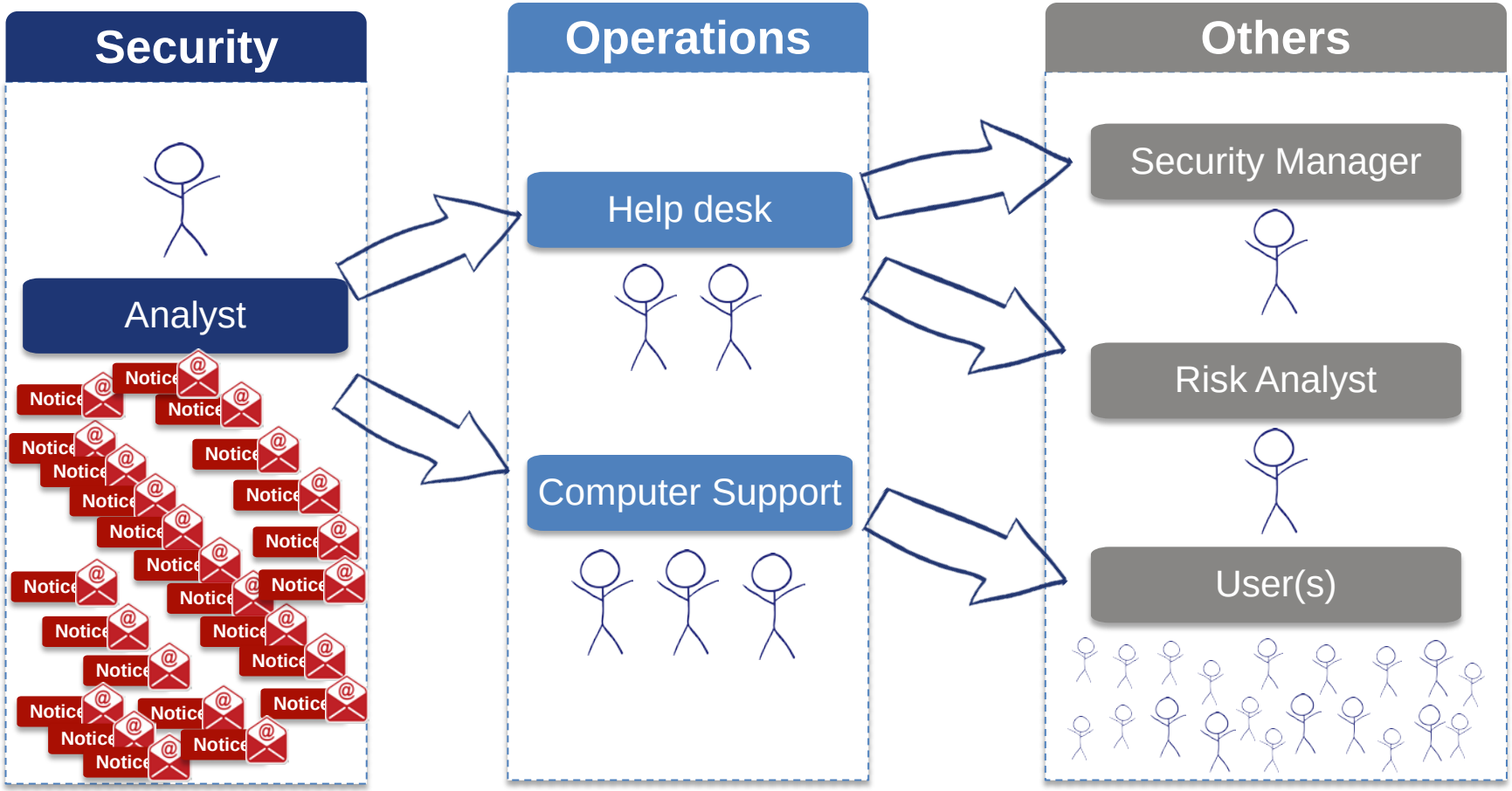
Identified security event which requires action

Incident

- **Investigation**
- **Trouble Ticket**
- **Incident Response**

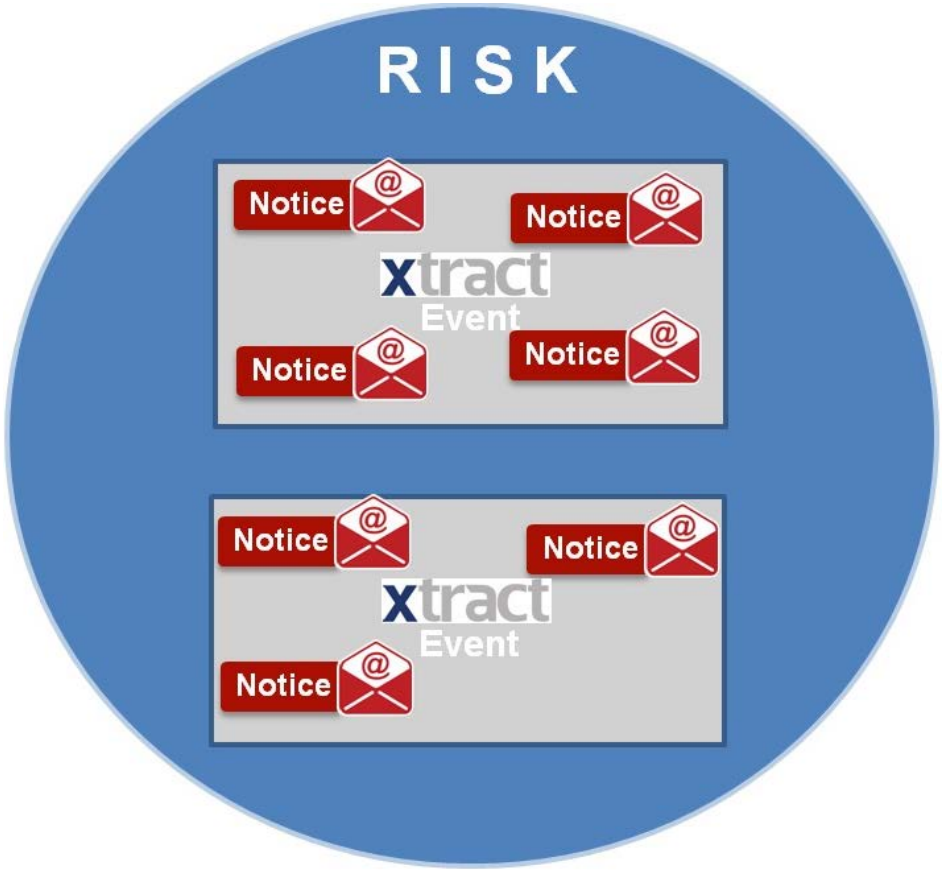
xtract ***uses Notices to create Events with sufficient information for a Security Analyst to determine if an Incident has occurred.***

Costs Associated with an Incident



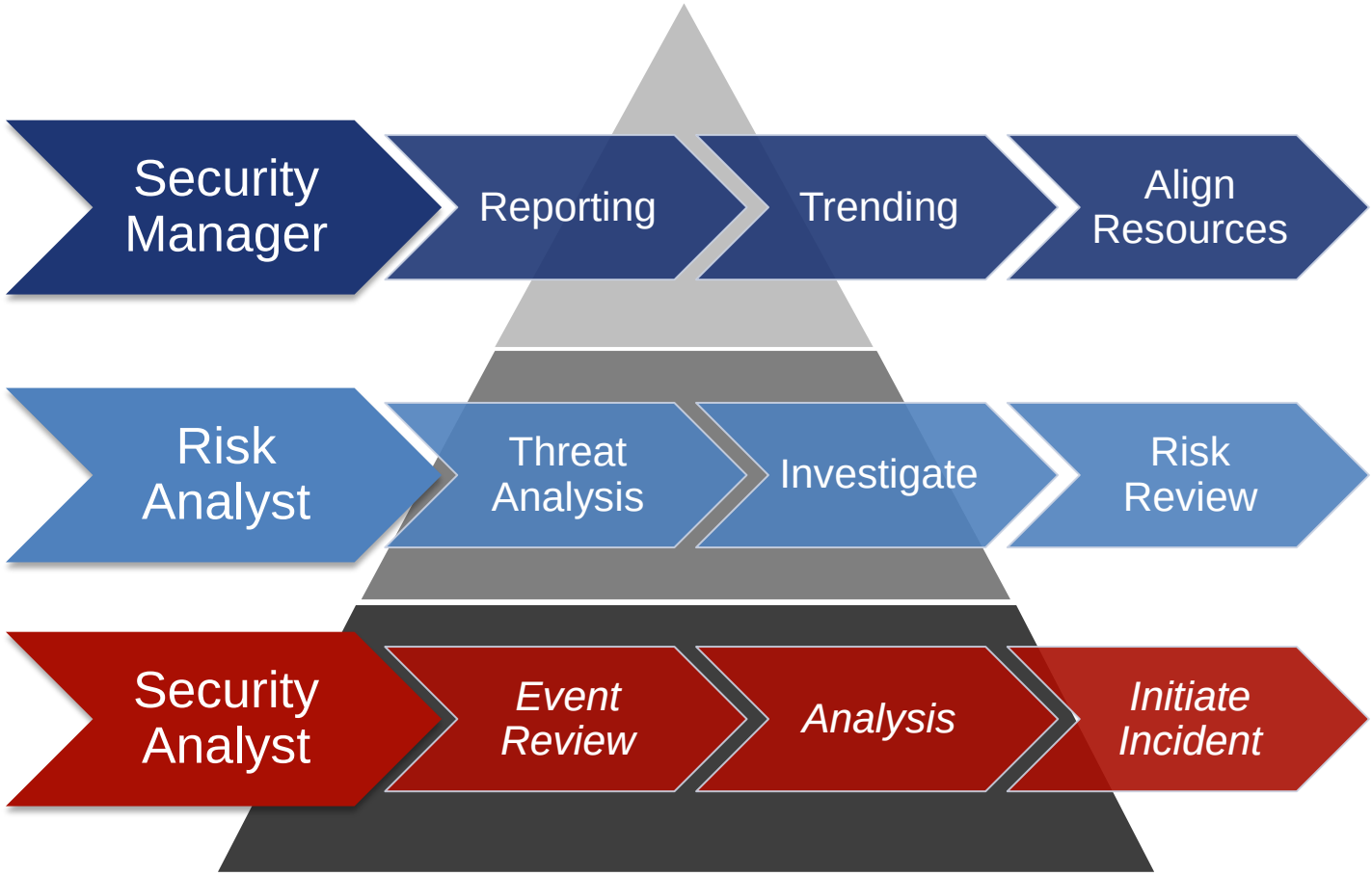
An Incident can trigger cascading work for users across divisions, so <u>false</u> positive identification of Incidents reduces costs.

Terminology: Notices, Events & Risks



Multiple notices can comprise an event. Use xtract to search across all events and notices to identify higher level Risks to the Enterprise.

Continuous Monitoring Strategy



xtract ***provides different views to align with NIST 800-137.***

Summary

Short term

- Ability to assess **all** potential threats (instead of sampling), without hiring more resources
- Reduces labor necessary to assess actual threat
- Improves relationships in organizations by targeted remediation instead of endless destruction of hard drives
- Enables customized, metrics-driven strategic risk management, tailored to each institution's needs

Long term

- Significantly improves threat analysis and assessment rather than simple repetitive incident response
- Enables institutional behavior/policy change based on analytics

So, what can it do for my Organization…

Securely Developed Application

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validator, Encoder
A2. Injection Flaws	Encoder
A3. Malicious File Execution	HTTPUtilities (Safe Upload)
A4. Insecure Direct Object Reference	AccessReferenceMap, AccessController
A5. Cross Site Request Forgery (CSRF)	User (CSRF Token)
A6. Leakage and Improper Error Handling	EnterpriseSecurityException, HTTPUtils
A7. Broken Authentication and Sessions	Authenticator, User, HTTPUtils
A8. Insecure Cryptographic Storage	Encryptor
A9. Insecure Communications	HTTPUtilities (Secure Cookie, Channel)
A10. Failure to Restrict URL Access	AccessController

xtract *implements OWASP ESAPI library.*

xtract

xta Threat Reduction, Analysis & Correlation Tool.

DEMONSTRATION

Sample Email Notice

DATE/TIME (UTC) = 12/1/2014 11:07:10

PROTO = TCP

SAFE HIT SRCIP = 100.100.101.23

SRCPORT = 7555

DESTIP = 1.2.3.4

DESTPORT = 80

CUSTOMER DNS LOOKUP SRCIP = 10.8.8.12

REF# = abcd1234

Event Analysis

xtract
xla Threat Reduction, Analysis & Correlation Tool.

Timestamp	User	Src	Dst	URL	Status	Sent	Rcvd
7/1/14 9:12:01	mplanck	192.168.0.10	**1.2.3.4**		allowed	0	0
7/1/14/ 9:12:00	mplanck	192.168.0.10	80.0.1.12	google.com	allowed	1022	4320
7/1/14 9:11:59	mplank	192.168.0.10	12.2.6.8	hacker.com	blocked	0	0
7/1/14 9:11:59	mplank	192.168.0.10	52.1.1.12	malware.com	allowed	120	1409928

Use Excel's built-in sorting and filtering features to identify risks: downloaded .exe files, large uploads, connections to strange domains or other suspicious patterns of behavior

A Security Analyst can view network traffic before & after the notice to investigate the cause and effect and determine if an Incident has occurred.

Event Review

Analysis | Reporting | Admin

Time Frame | View | Actions | Search | Advanced

Incident	#	Sev	Notes	First Date	Last Date
	1		testing	08/20/2014 12:06:04	08/20/2014 12:06:04
	2			08/08/2014 17:07:56	08/08/2014 17:07:56
	2		N/A	08/07/2014 15:47:58	08/07/2014 15:48:06
	2			08/07/2014 10:37:42	08/07/2014 10:37:42
	1		N/A	08/04/2014 15:58:59	08/04/2014 15:58:59
	1		N/A	08/04/2014 10:48:53	08/04/2014 10:48:53
	2		N/A	07/24/2014 11:51:48	07/24/2014 11:56:41
	3		N/A	07/16/2014 17:15:37	07/16/2014 17:17:05
	2		incident refered to HR	07/16/2014 14:59:06	07/16/2014 14:59:06
	3		trouble ticket #01124	07/14/2014 20:48:19	07/14/2014 20:49:25

Notices Log

Analysis | Reporting | Admin

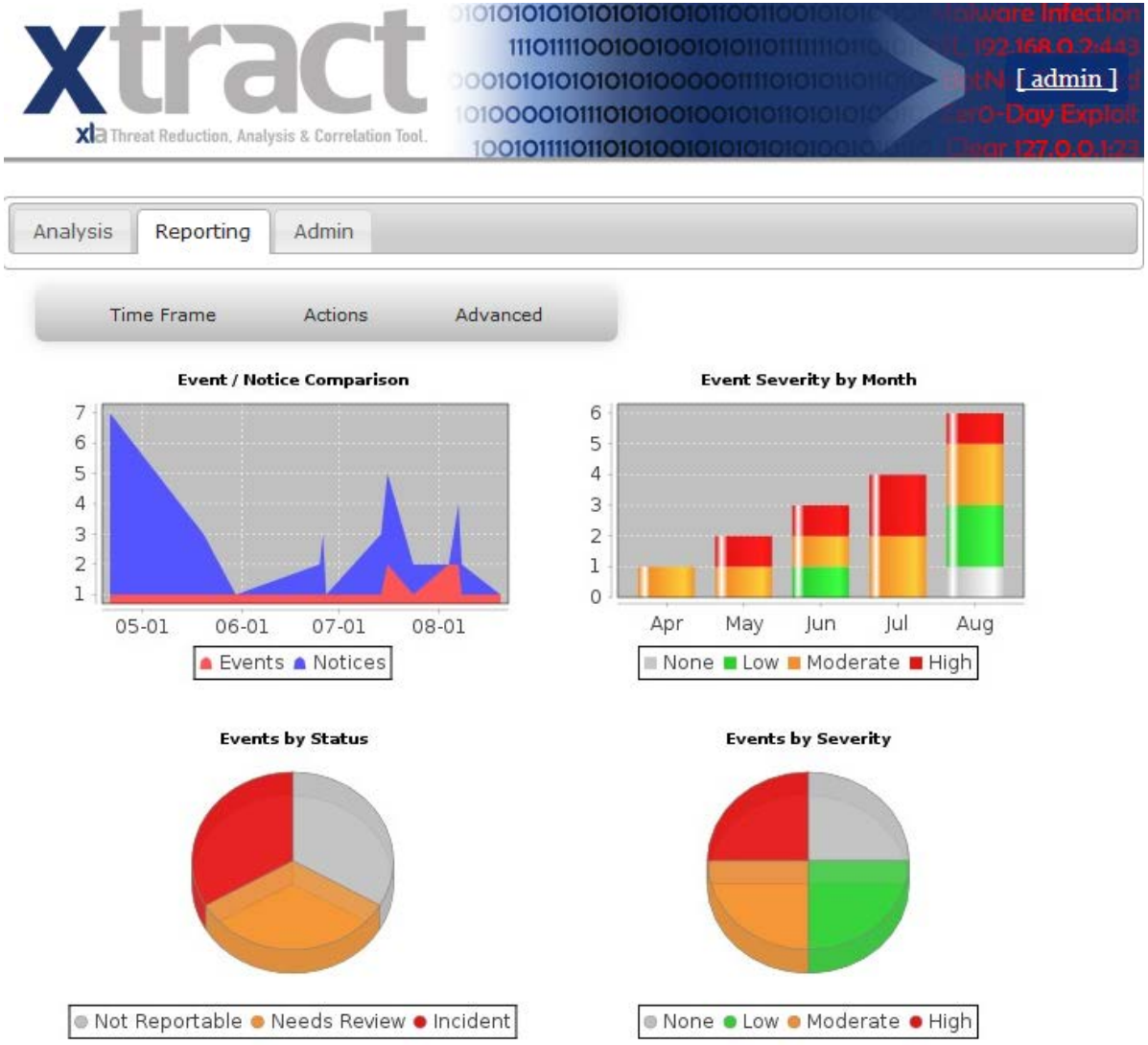
Time Frame | View | Actions | Search | Advanced

Sev	Total	Ref #	First Date	Last Date	Notes	Notices
	18	SAFE Hit Only	04/21/2014 14:23:48	08/20/2014 12:06:04	testing with really really long not...	*[show]*
	5	abc123	06/26/2014 12:53:51	08/08/2014 17:07:56	n/a	*[show]*
	4	1z2x3c4v	07/14/2014 20:48:19	08/07/2014 15:47:58	notest here	*[show]*
	3	1234567	04/21/2014 14:23:42	04/21/2014 14:23:49	n/a	*[show]*
	2	tyruei123	08/04/2014 10:48:53	08/04/2014 15:58:59	suspicious activity	*[show]*
	2	op908i7	07/24/2014 11:51:48	07/24/2014 11:56:41	n/a	*[show]*
	1	zyxvwut	07/16/2014 17:15:37	07/16/2014 17:15:37	n/a	*[hide]*

Date/Time	Hit Type	Source	Destination	Users	Download
07/16/2014 17:15:37	DNS with SAFE Hit	192.168.3.216	1.2.3.10:80	CPTOLEMY	

	1	abcdefg	05/30/2014 15:38:07	05/30/2014 15:38:07	testing low	*[show]*

Reporting Features



FOR MORE INFORMATION PLEASE CONTACT:

xtract@xla.com