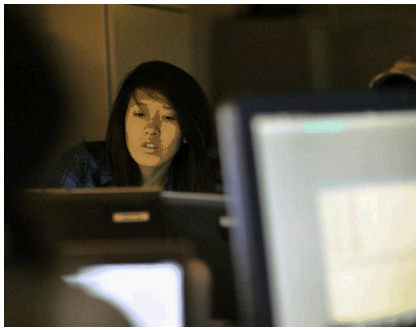
SAND2014-18613PE

Exceptional service in the national interest

Sandia National Laboratories





Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams

Theodore Reed, Robert G. Abbott, Benjamin Anderson,
Kevin Nauer & Chris Forsythe

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Cyber threats pose a major risk to business, government and other organizations

Sandia National Laboratories

Chicago Tribune
News

Chinese hackers steal data from 4.5 million patients in U.S. hospital chain

By Cynthia Koons and Michael Riley, Bloomberg News, Bloomberg

CNN Money

Video

Home | Business | Markets | Investing | Economy | Tech | Personal Finance

The Cybercrime Economy

Data breach at UPS Stores in 24 states

By Charles Riley @CRrileyCNN August 21, 2014: 8:10 AM ET

THE WALL STREET JOURNAL.

BUSINESS

Target Hit by Credit-Card Breach

Customers' Info May Have Been Stolen Over Black Frida

Email | Print | 24 Comments

By ROBIN SIDEL, DANNY YADRON and SARA GERMANO CONNECT

Updated Dec. 19, 2013 7:29 a.m. ET

REUTERS EDITION: U.S.

HOME | BUSINESS | MARKETS | WORLD | POLITICS | TECH | OPINION | BREAKINGVIEWS

USA TODAY
A GANNETT COMPANY

Search

NEWS | SPORTS | LIFE | MONEY | TECH | TRAVEL | OPINION | 76° | CROSSWORDS | YOUR TAKE | INVESTIGATIONS | VIDEO | STOCKS | MORE

P.F. Chang's: 33 restaurants affected in data breach

Derry London, WLTX 10:59 a.m. EDT August 4, 2014

Scottsdale, AZ (WLTX) -- The restaurant chain P.F. Chang's China Bistro said Monday a security breach first reported in June may have led to the theft of customer data from credit and debit cards used at

EBay asks 145 million users to change passwords after cyber attack

BY JIM FINKLE, SOHAM CHATTERJEE AND LEHAR MAAN

BOSTON/BANGALORE | Wed May 21, 2014 4:25pm EDT

12 COMMENTS | Tweet 1,075 | Share 244 | Share this | 92 | Email | Print

TECHNEWSWORLD

CYBERSECURITY

Computing | Internet | IT | Mobile Tech | Reviews | Security | Technology

TechNewsWorld > Security > Cybersecurity | Next Article in Cybersecurity

In Google Attack Aftermath, Operation Aurora Keeps on Hacking

The Operation Aurora hackers, who compr
Google's infrastructure a few years ago, ar
targeting defense contractors and other co
their supply chains. The group is persistent
sophisticated and most likely government-s
said Grayson Milbourne, director of threat r
Webroot.

COMPUTERWORLD

White Papers | Webcasts | New

Topics | News | In Depth | Reviews | Blogs | Opini

Applications | App Development | Big Data | Business Intelligence/Analyti | Emerging Technologies | Enterprise Architecture | ERP | Unified Communications

Home > Applications > Desktop Apps

News

Evernote hit by denial of service attack

The attack temporarily shut down Evernote, which now has over 1 million users

By Tim Hornyak

June 11, 2014 05:57 AM ET | Add a comment

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER

ATTACKS/BREACHES

7/28/2011 11:55 AM

RSA SecurID Breach Cost $66 Million

EMC details second quarter 2011 cost to replace tokens, monitor customers, and handle fallout from RSA's SecurID breach.

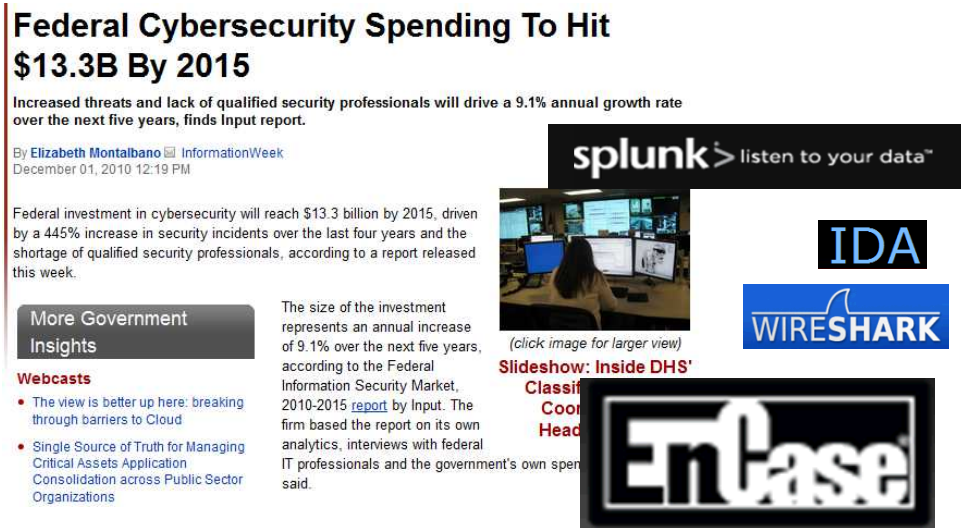
Mathew J.

Between April and June 2011, EMC spent $66

Despite extensive investments in technology, the human remains the last line of defense

Sandia National Laboratories

- Intrusion detection, firewalls, email filters, anti-virus and other technologies stop most cyber threats
- Yet, criminals still find backdoors and vulnerabilities that provide a foothold onto IT networks
- Humans must fill the gap between the capabilities of technologies and those of adversaries who are sophisticated, enterprising, well-connected, motivated and persistent



Federal Cybersecurity Spending To Hit $13.3B By 2015

Increased threats and lack of qualified security professionals will drive a 9.1% annual growth rate over the next five years, finds Input report.

By Elizabeth Montalbano InformationWeek
December 01, 2010 12:19 PM

Federal investment in cybersecurity will reach $13.3 billion by 2015, driven by a 445% increase in security incidents over the last four years and the shortage of qualified security professionals, according to a report released this week.

More Government Insights

Webcasts

- The view is better up here: breaking through barriers to Cloud
- Single Source of Truth for Managing Critical Assets Application Consolidation across Public Sector Organizations

The size of the investment represents an annual increase of 9.1% over the next five years, according to the Federal Information Security Market, 2010-2015 report by Input. The firm based the report on its own analytics, interviews with federal IT professionals and the government's own spen said.

(click image for larger view)

Slideshow: Inside DHS'
Classif
Coor
Head

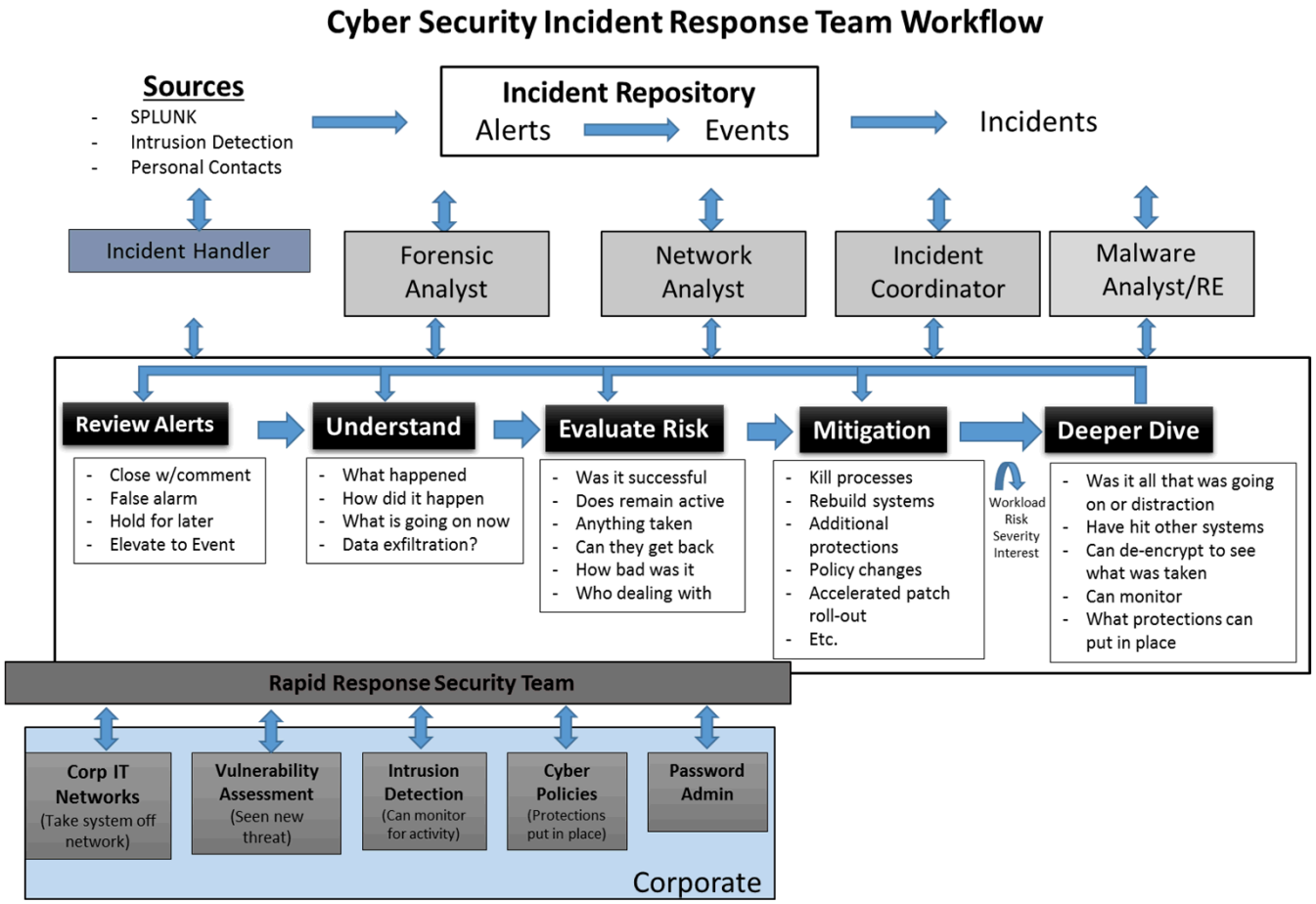
splunk> listen to your data™

IDA

WIRESHARK

EnCase

Cyber Security Incident Response Teams (CSIRTs) serve as frontline defenders

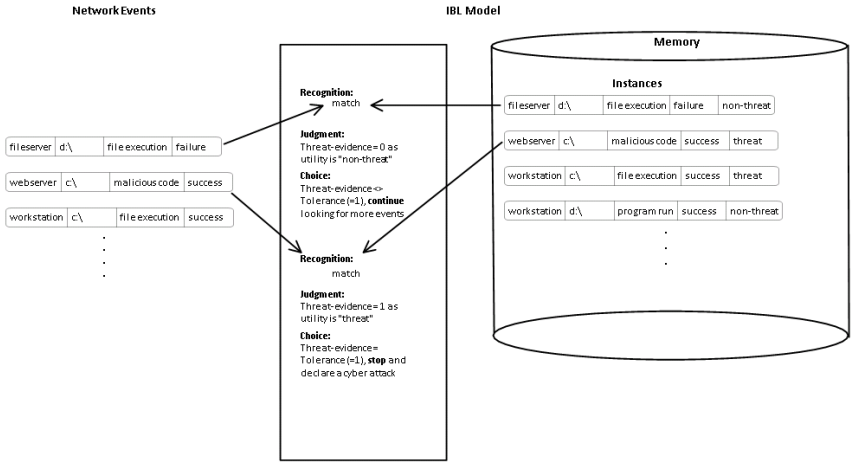


- Assess alerts and conduct forensic analysis to identify, mitigate and defend against cyber threats
- Priorities, practices and make-up vary across organizations
- Utilize an array of commercial and homegrown software tools for forensic analysis, and archiving and searching past incidents

Existing models have focused on high-demand, as opposed to everyday operations

- ACT-R model incorporated risk aversion and experience with threats, *Dutt, Ahn & Gonzalez (2013)*
- Agent-based model of two-way interaction between attackers and defenders, *Kotenko, 2005*
- Game theory-based simulation of inferences made by attackers and defenders, *Hamilton & Hamilton, 2008*
- Models focused on adversary tactics, *Eom et al., 2008; Lee et al., 2005; Zakrzewska & Ferragut, 2011*

Excerpt from ACT-R Model of Cyber Defenders



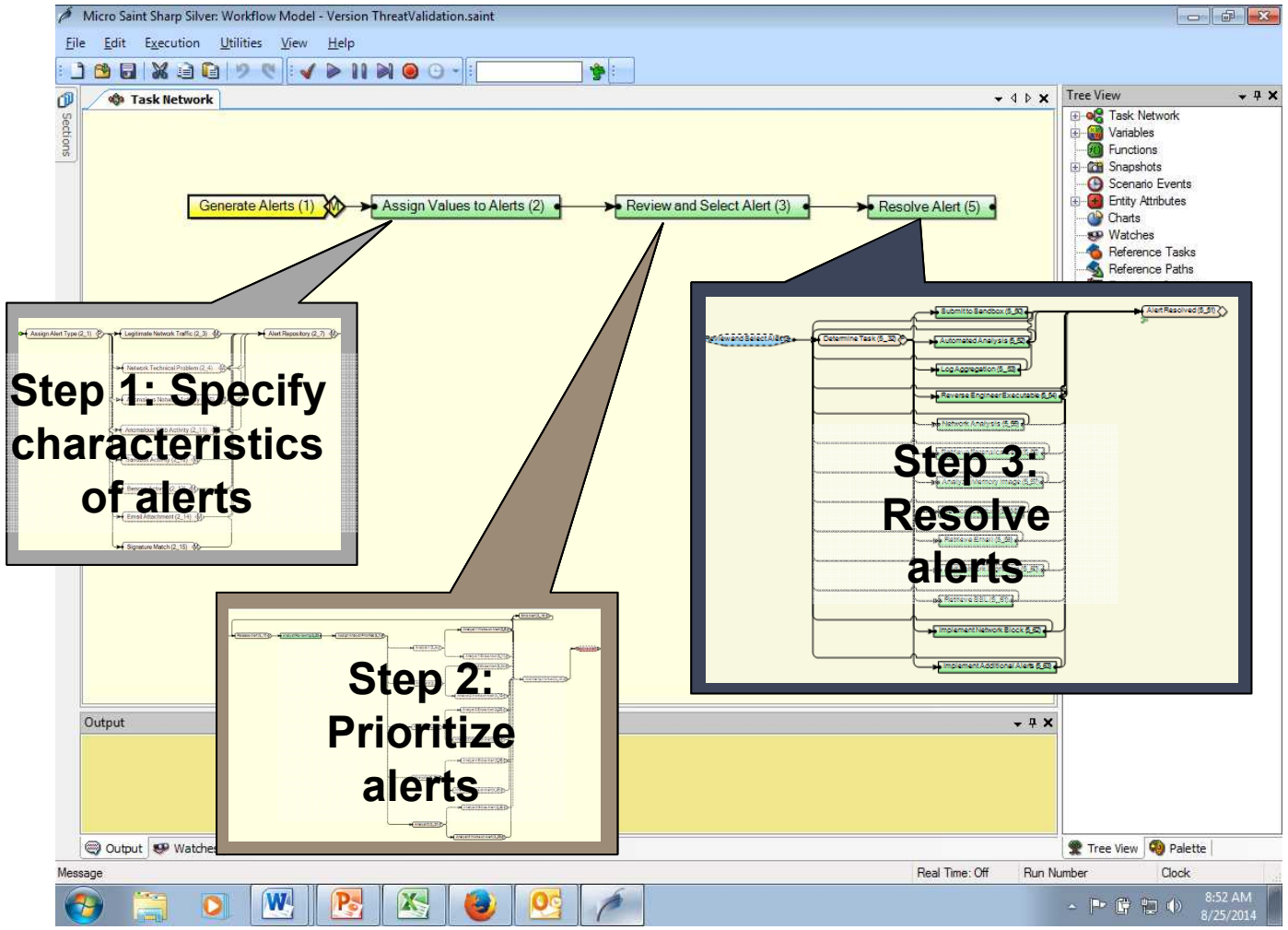
From Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*(3), 605-618.

Model of operations enables comparison of alternative tools, practices, staffing, etc.

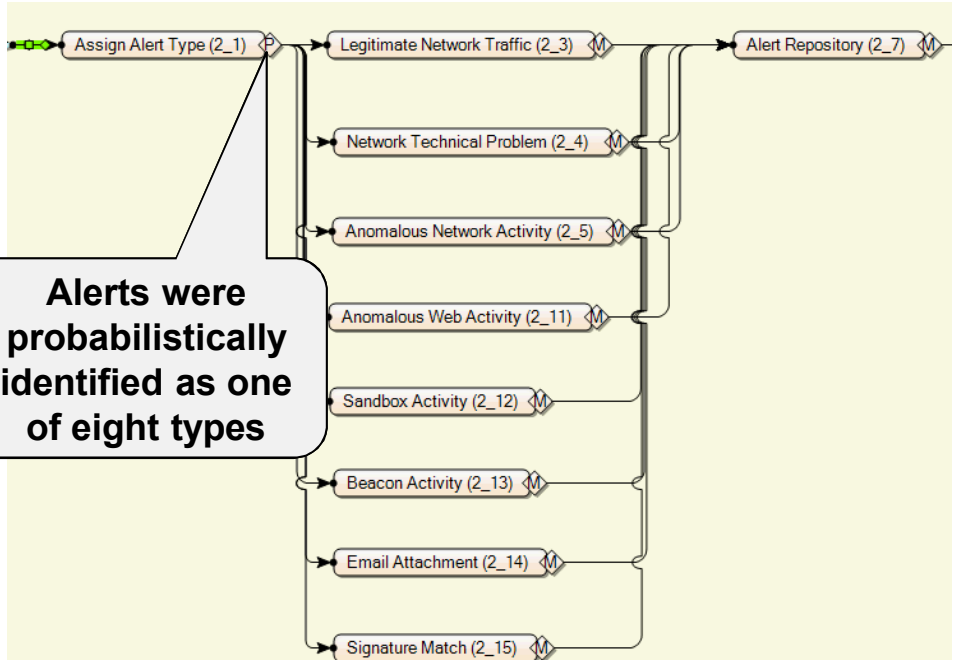
Sandia National Laboratories

CSIRT workflow modeled as a discrete event simulation using MicroSAINT Sharp

NOTE: The objective was to model workflow, as opposed to developing a cognitive model.

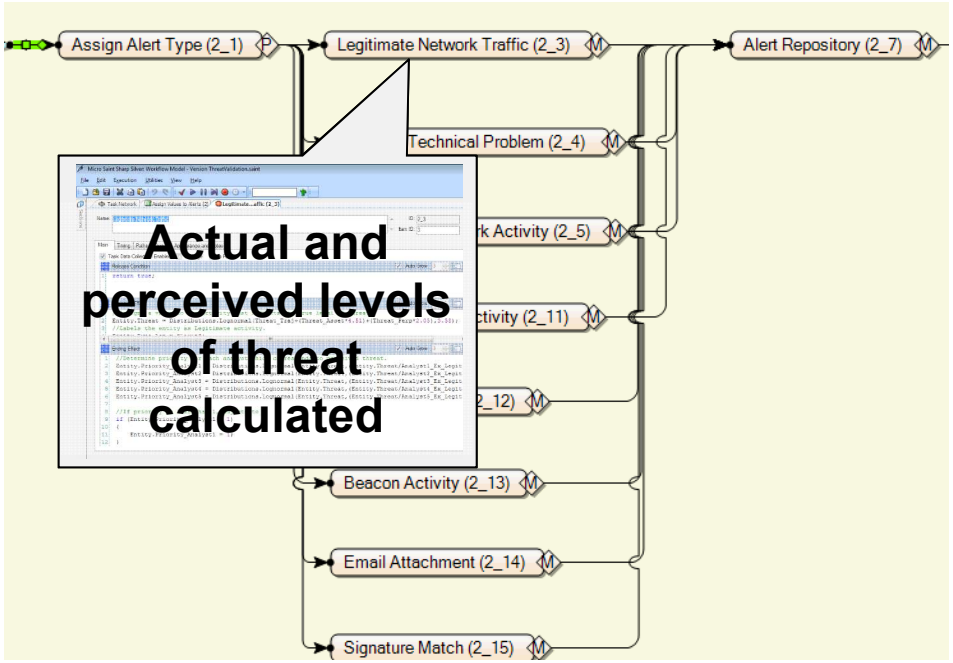


Alerts were generated and their characteristics specified



- Overwhelming majority of alerts result from either:
  - Legitimate user behavior,
  - Technical problems unrelated to cyber security, or
  - False alarms generated by automated monitoring
- Likelihood of each alert type was based on actual data
- Simulated daily experience of arriving in the morning with a queue containing alerts either generated overnight or left over from the day before

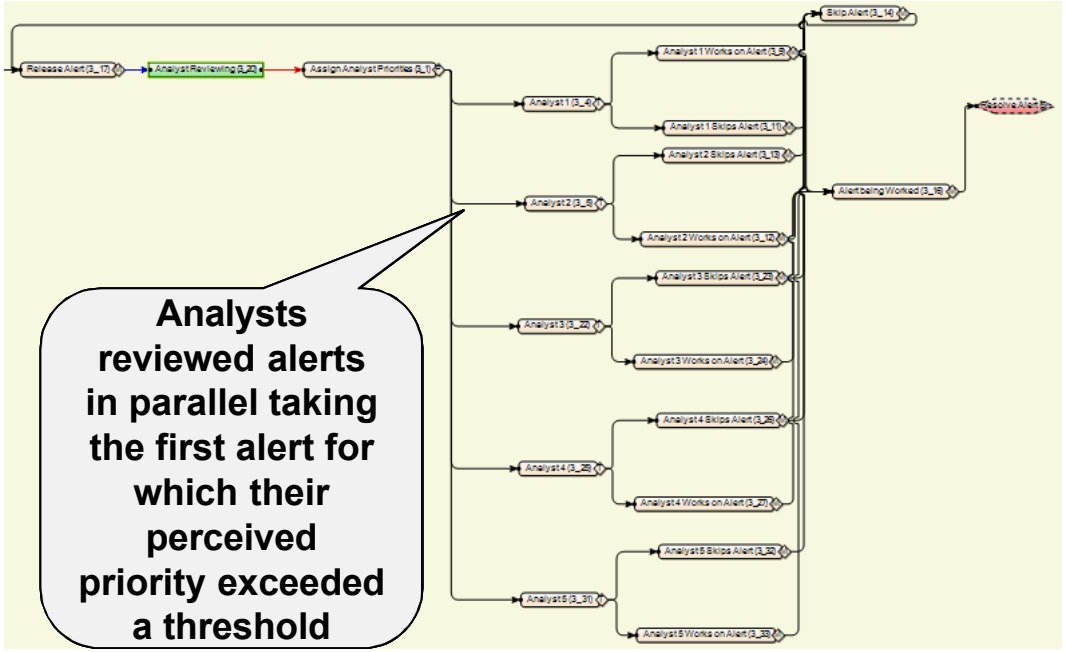
Given the type of activity, ground truth level of threat and perceived priority were specified



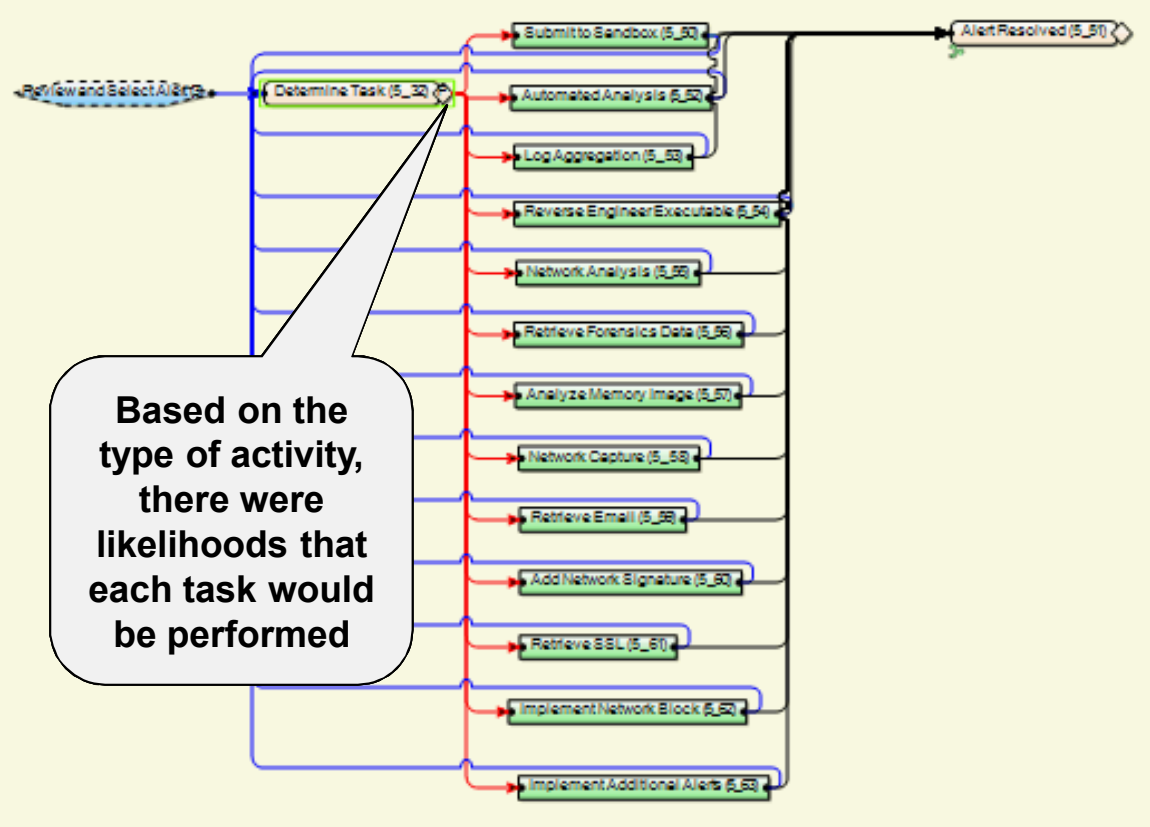
- Threat characteristics were specified:
  - Trajectory of the attack
  - Asset targeted
  - Perpetrator
- Based on threat characteristics, a value was derived for the ground truth level of threat
- Perceived priority was calculated as a function of ground truth and characteristics of individual analysts
  - Related domain knowledge
  - Related experience

Analysts selected alerts for investigation from the queue

- Current model simulated a CSIRT consisting of five analysts
- In parallel, analysts skimed the queue searching for an alert for which their perceived priority exceeded a pre-specified threshold, taking the first alert that exceeded this threshold
- If no alerts met this criteria, the threshold was lowered and the process repeated

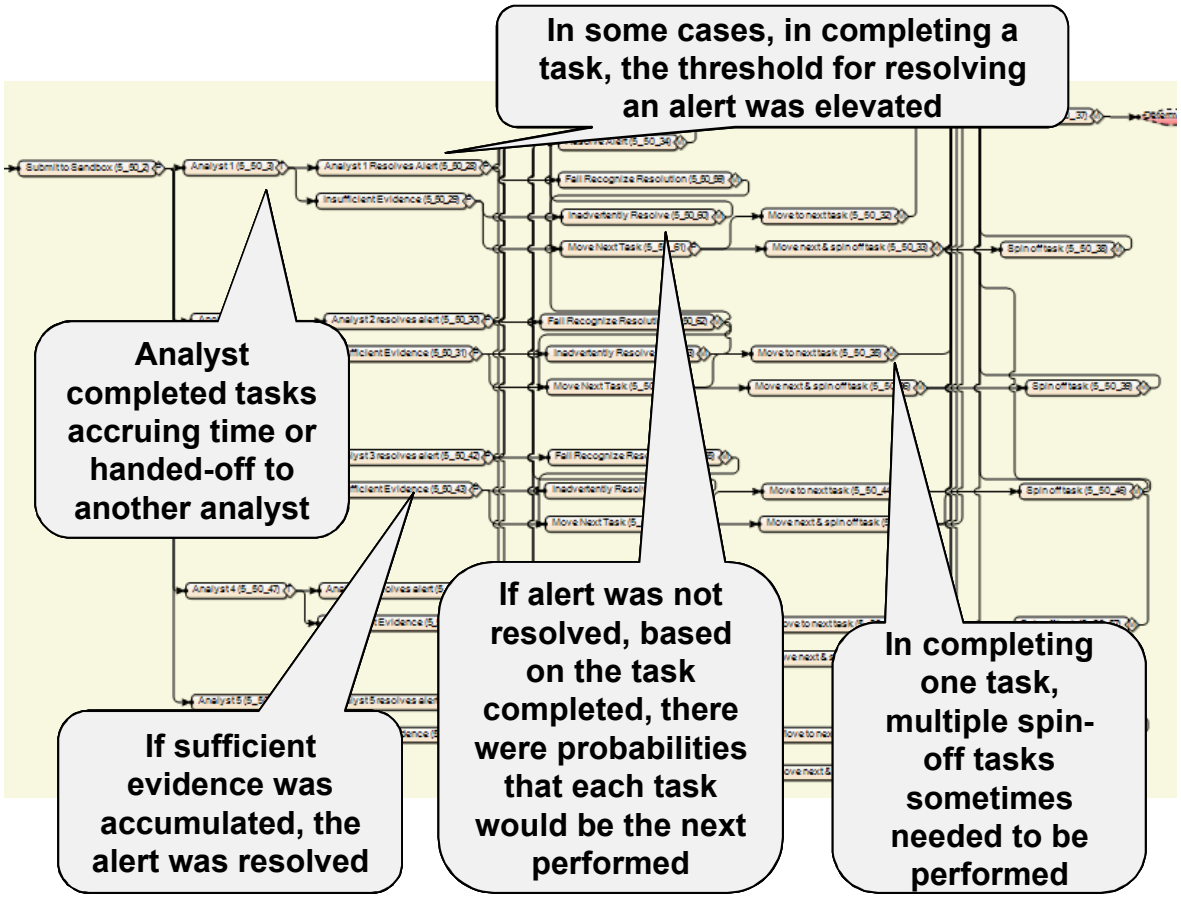


Once an alert was selected from the queue, the investigation began



- Analysts performed one of thirteen forensic analysis tasks
- Forensic analysis tasks corresponded to the use of different software tools
- Based on the type of activity, there was a likelihood based on logs of actual events that each task would be performed

Through tasks, evidence was accumulated toward the resolution of an alert



- The time to perform a given task was drawn from a random distribution of times for the type of task
- Analysts sometimes selected to hand off a task to another analyst with superior knowledge or experience
- Tasks generated evidence and once sufficient evidence was accumulated, the alert was resolved

Validation involved generating alerts equivalent to a set of actual alerts

Sandia National Laboratories

- A set of 136 alerts and associated records were obtained and an equivalent set of alerts generated with the simulation
- The threat characteristics of each alert were rated using the MITRE Cyber Prep Methodology, Mateski et al. (2012)
  - Trajectory
    - (1) targeting no specific entity,
    - (2) targeting a specific single entity, or
    - (3) targeting multiple entities or high-value entities
  - Targeted asset
    - (1) no asset,
    - (2) a client or set of client assets, or
    - (3) an infrastructure, service, or critical asset
  - Perpetrator
    - (1) a careless or unknown entity,
    - (2) an action associated with criminal activity, or
    - (3) an action associated with an advanced threat
- Two cyber security forensic analysts rated alerts,

  Interrater reliability = 77% (r = 0.580; p<0.0001

Each threat characteristic was correlated with measures of the level of effort

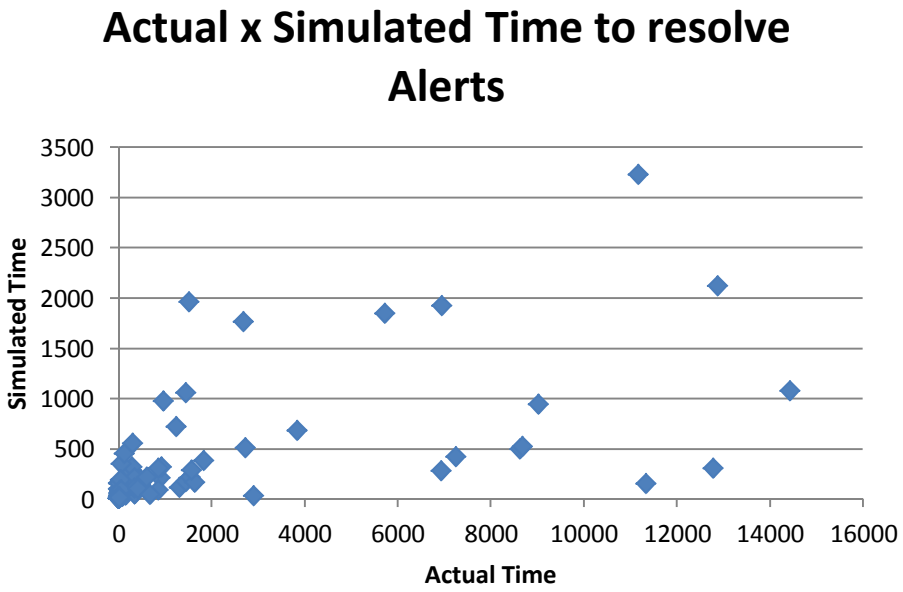
- Records provided three measures of the level of effort required to resolve alerts
  - Total time
  - Number entries
  - Number analysts

	Total Time	# Entries	# Analysts	Trajectory	Asset
# Entries	r=0.513 p<0.001				
# Analysts	r=0.524 p<0.001	r=0.860 p<0.001			
Trajectory	r=0.171 p<0.048	r=0.348 p<0.001	r=0.229 p<0.008		
Asset	r=0.326 p<0.001	r=0.352 p<0.001	r=0.311 p<0.001	r=0.241 p<0.005	
Perp	r=0.171 p<0.048	r=0546 p<0.001	r=0.498 p<0.001	r=0.192 p<0.026	r=0.136 NS

- Measures of the level of effort required to resolve alerts were correlated with one another and ratings for each threat characteristic
- Correlations between the ratings for threat characteristics varied

Model predictions for the time to resolve alerts correlated with actual times

- Alerts generated with the same characteristics as actual alerts
- For the simulation, analysts were assigned an intermediate level of expertise
  - (Expertise = 5, on a scale of 1-10)
- NOTE: Simulation did not account for analysts suspending work on an alert and resuming work at a later time



r=0.185, p<0.03

NOTE: Time units are notional values and do not reflect actual units of time

Conclusions and afterthoughts

Sandia National Laboratories

- The model appears to capture the basic mechanics that determine the workflow within a CSIRT
- Questions may be raised concerning the differential contribution of threat characteristics, and the knowledge and experience of analysts to the time to resolve alerts
- Knowledge and experience are believed to influence workflow in three ways
  - (1) As analysts gain expertise, they more accurately assess the nature of threats and are better able to calibrate the level of effort devoted to an individual alert to the threat posed by the event
  - (2) A richer understanding of tasks should allow analysts to perform those tasks more efficiently and productively
  - (3) Greater knowledge of the procedures entailed in using software tools combined with a better conceptual knowledge of the application of the software tools should result in superior efficiency and productivity