RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Accelerate Your Security Operations With Machine Speed Responses to Cyber Attacks

SESSION ID: SPO-T08

Bernie Thomas

Principal Security Architect
CSG Invotas
@csginvotas

#RSAC

Barriers to Speed…

- Attack surface continues to grow in parallel with technology adoption – more to protect
- We can’t keep up! - Staff headcount isn’t keeping pace with the increasing incident volumes – never enough trained staff
- Explosion in specialty point solutions increases complexity and limits agility of response – tools, tools and more tools…
- Attackers don’t have to deal with politics and bureaucracy….

Breaches Take Too Long to Fix

More than one-third report that security events typically take hours to detect and diagnose. The majority indicate that resolution takes days, weeks, or even months.

Time Spent on Each Process Ensuing a Security Event

	Seconds	Minutes	Hours	Days	Weeks	Months	Don’t know
Detection	10%	29%	35%	11%	2%	6%	7%
Diagnosis	3%	11%	48%	25%	4%	3%	6%
Resolution	1%	9%	30%	37%	13%	4%	6%

From IDG Research Services conducted January 2014

Why Is Response Slow?

What consumes

a SOC analyst’s time?

Approvals

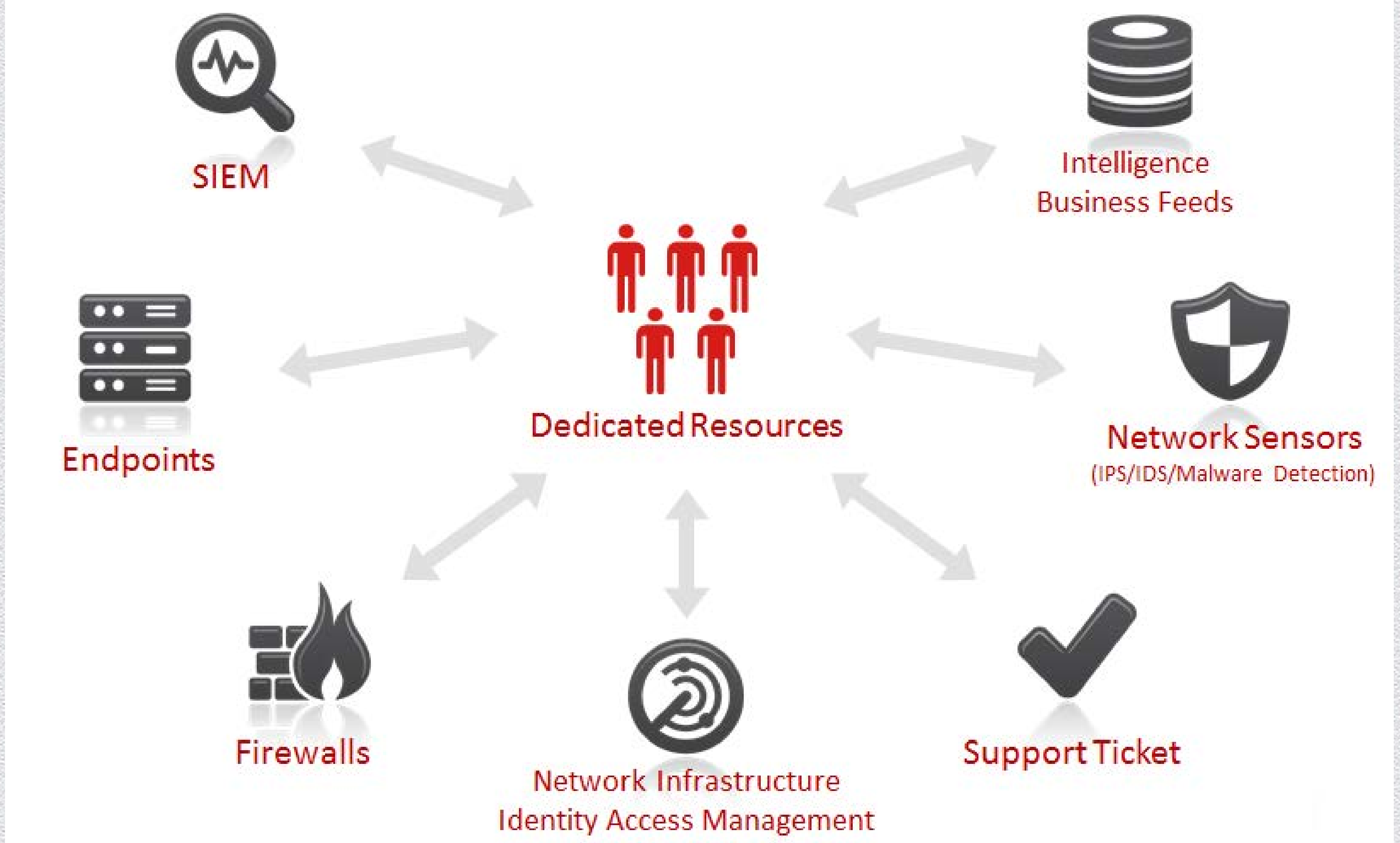
Opening, updating and closing trouble tickets

Manually moving from one tool to another

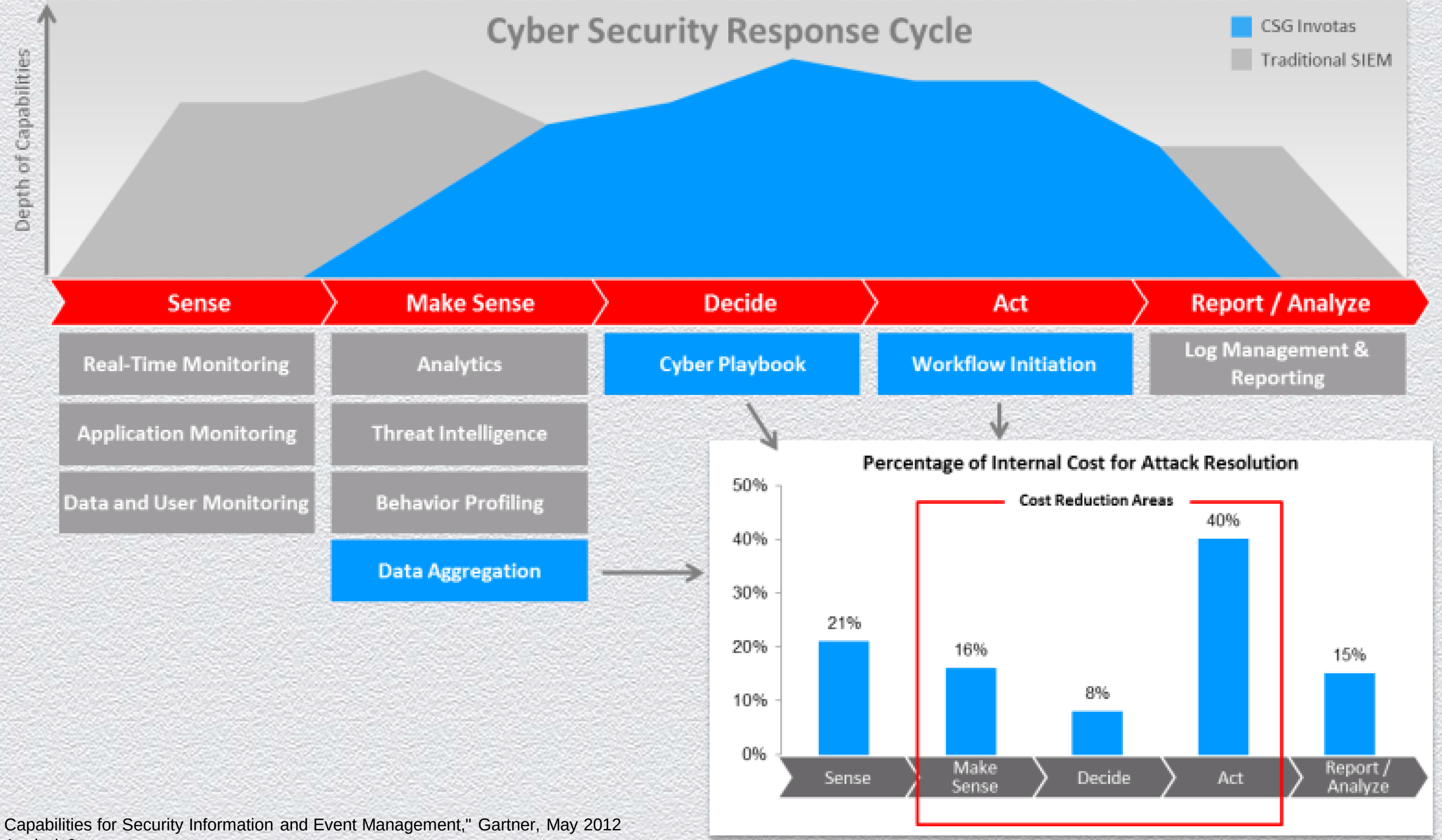
Meetings

Email

Current Operational Environment



Where Can We Improve?



Sense	Make Sense	Decide	Act	Report / Analyze
Real-Time Monitoring	Analytics	Cyber Playbook	Workflow Initiation	Log Management & Reporting
Application Monitoring	Threat Intelligence			
Data and User Monitoring	Behavior Profiling			
	Data Aggregation			

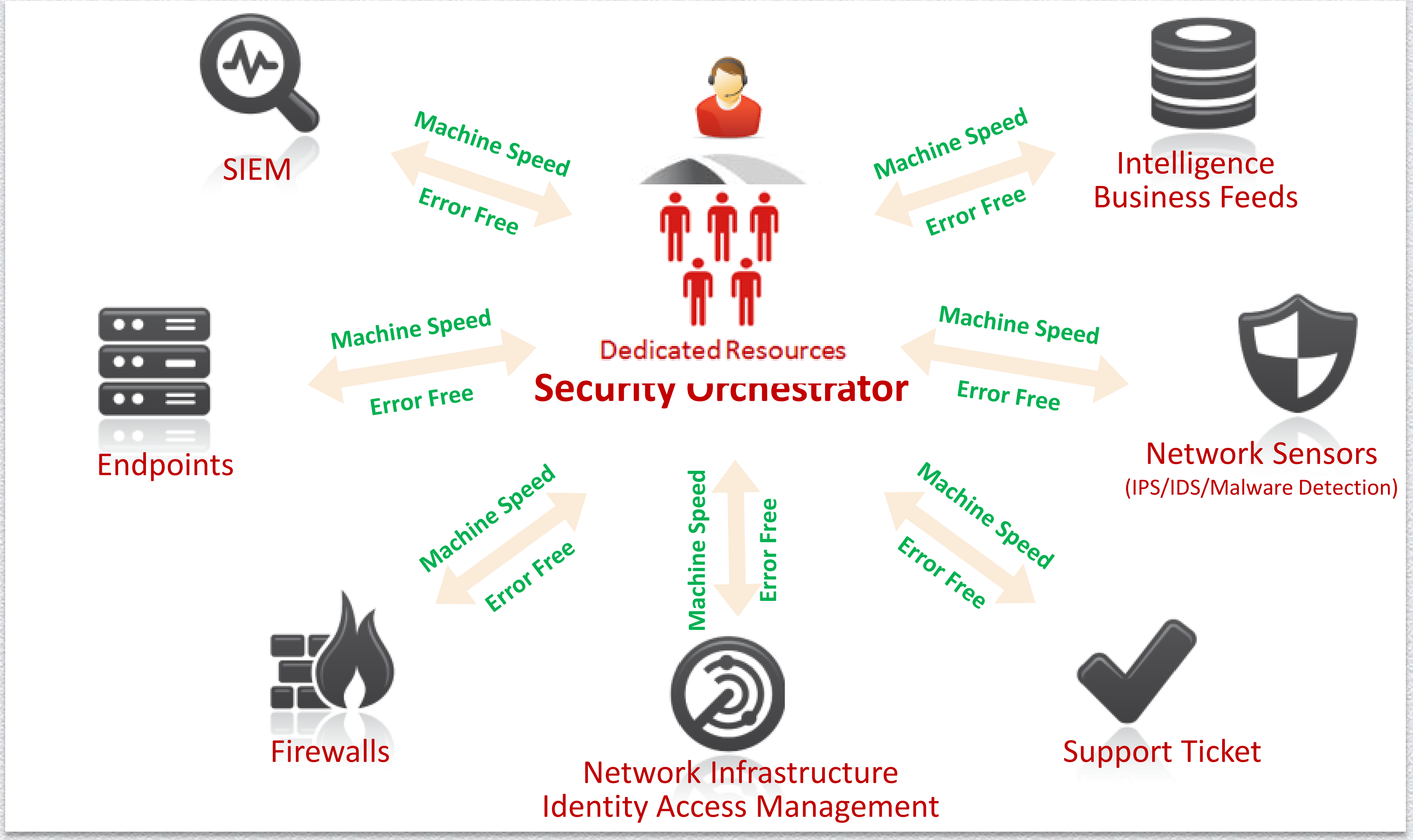
Sources:
1. “Critical Capabilities for Security Information and Event Management," Gartner, May 2012
2. Deloitte Analysis0

How Can We Improve?

Security Orchestration

Immediate, Interoperable, Real-Time

Current Operational Environment



Orchestration

The Next Evolution of Cyber Security

- Easily manage responses to attacks with large volumes and complexity, with fewer resources
- Respond to and contain attacks in seconds, minimizing potential damage, loss and risk
- Manage and protect from a “single pane of glass”
- Elevate your current staff to higher value services and reduce the cost and frequency of new hires

Simplicity Scales

Making Orchestration Practical for Everyday Use

Unification: Art of Managing Many

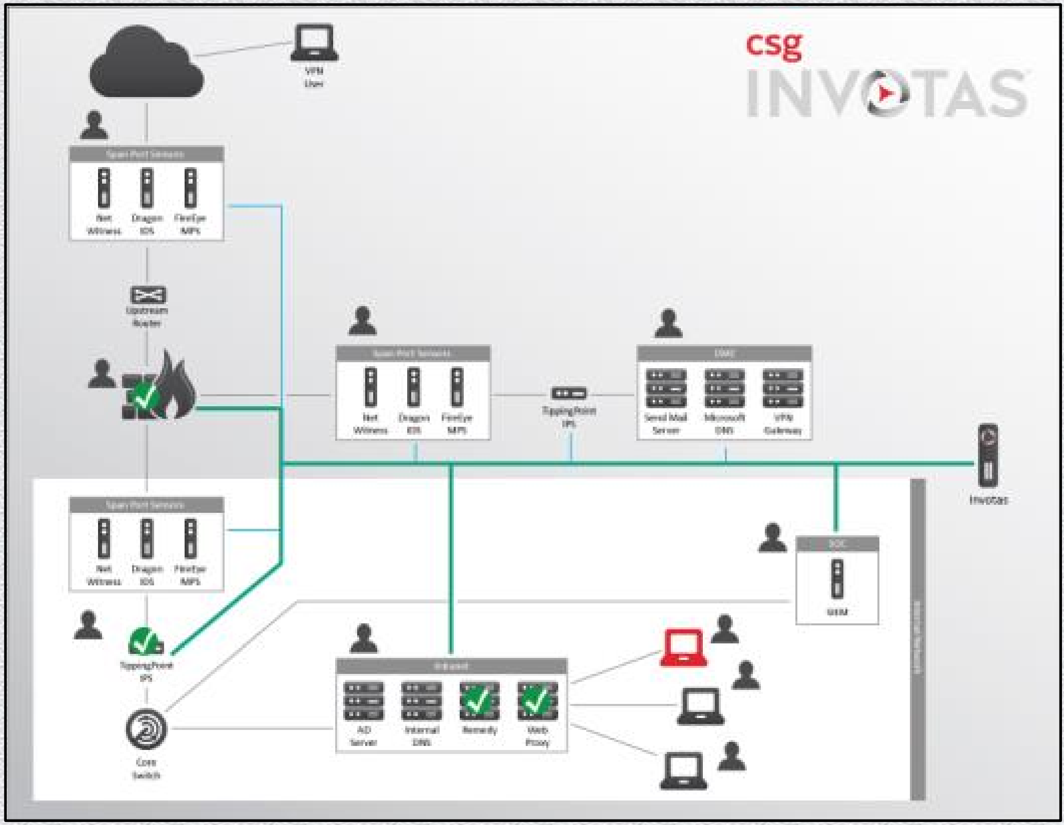
- Rarely does it take just one device or resource to respond to cyber attacks
- Analysts have to interface with each point solution separately
  - Required training for each tool
  - Tools are often siloed in different parts of the organization
  - These issues can cause delays in response time
- Here are just a few common tools:

Ticket Tracking	SIEM	Malware Detection	Firewall and VPN	Access Management	Mail Server	Network Forensics

- Having a unified approach using automation and orchestration for defensive strategies can save precious time and human capital

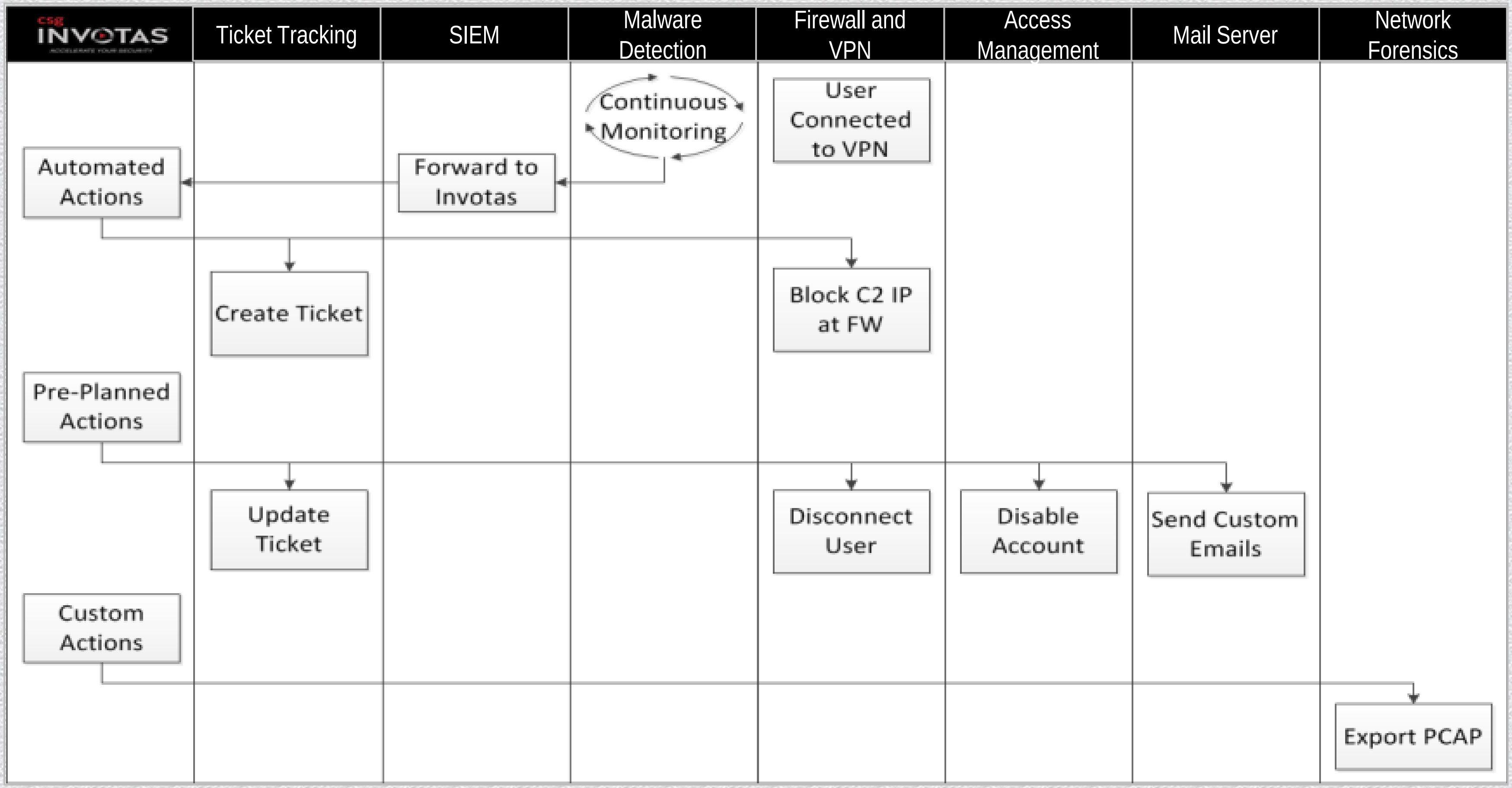
Security Unification Framework

- Unified Management, tying point solutions together
- Present relevant data quicker for event analysis
- Accelerate incident response with faster response
- Lower risk of human error
- Detailed audit trail of all actions taken is a must



Real World Example:

Protecting Against A Compromised VPN User



Analyzing the Results

Orchestration and Automation

- Current State for Infected VPN Users
  - Time from Identification to Resolution: 45 minutes
  - Occurs about 120 times per month = 90 hours
- Automation and Orchestration of the VPN Use Case
  - Time from Identification to Resolution: < 1 minute
  - Efficiency Gain: 98% efficiency gain in human time – (88 hours a month or ½ FTE)

Key Benefits

Automation and Orchestration

Security orchestration with automation helps CIOs to greatly reduce the time it takes to contain and mitigate security incidents by dynamically shifting the security state of the network at "machine speed."

And…It's cool.
It enables advanced security strategies

- Policy based behavior *throughout* the enterprise's systems
- Behavioral Scoring of actors
- Deception & Misinformation
- Automated Intelligence Gathering
- Decision Support

Key Benefits:

- **Unification of Action:** Synchronizes large-scale changes using controlled automation, with analyst-in-loop oversight
- **Cost Efficiencies**: Fewer personnel hours spent performing repetitive tasks means more hours spent actively defending networks
- **Speed & Effectiveness of Response**: Predetermined courses of action reduce time to contain compromises & thwart attacks
- **Accurate measurement**: Repeated actions can be audited, measured, perfected, and repeated

Questions?

How to Accelerate your Response to Attacks

Bernie Thomas
Principal Security Architect
bernie.thomas@csginvotas.com
@csginvotas