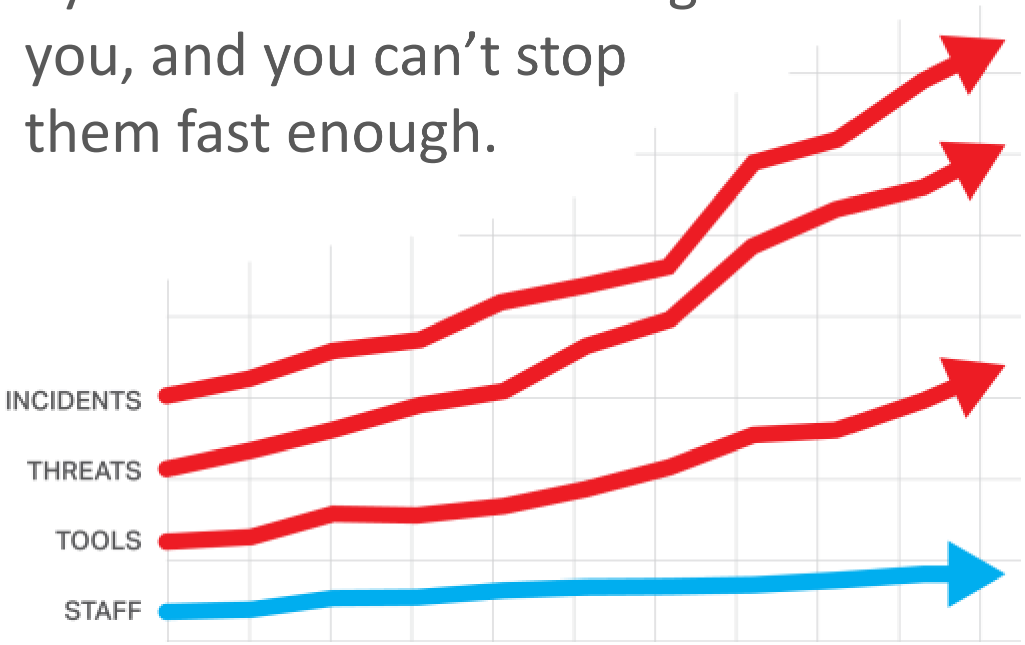
The Need for Speed

Understanding the Barriers to Speed and Leveraging Automation and Orchestration to Accelerate Your Security

Why Are You So Slow?

Cyber attacks are flooding you, and you can't stop them fast enough.



81% say the number of security events increased or remained the same in 2013.*

The number of tools and their complexity continue to increase.

Staffing levels remain the same to slightly higher.

It can take months to detect a threat. It can take days, weeks or months to resolve it.

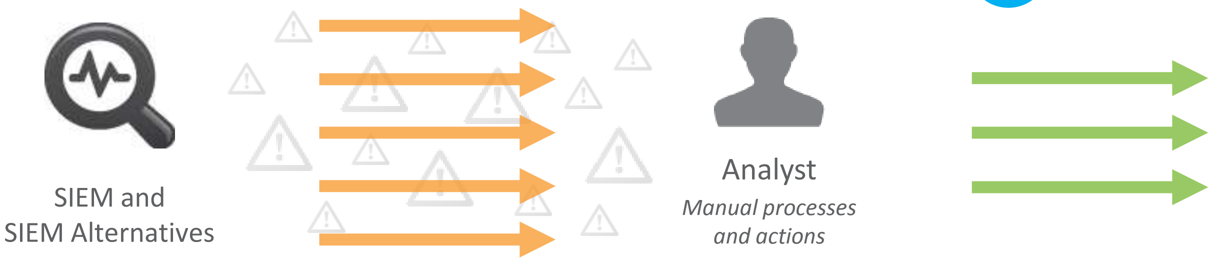
The longer it takes, the more you are exposed.

* Survey by IDG Research on security automation: info.csgi.com/idg-survey/

Alert Backlogs Increase Exposure

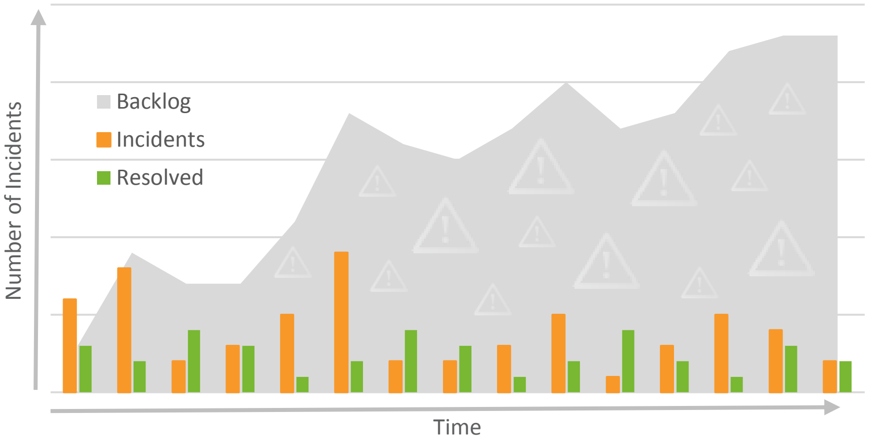
1 The SIEM is continuously reporting incidents for the Analyst to address.

2 Incidents often require 20 minutes to an hour to resolve.



Meanwhile … the SIEM continues to report incidents.

3 Inevitably a backlog develops and your network is increasingly exposed.



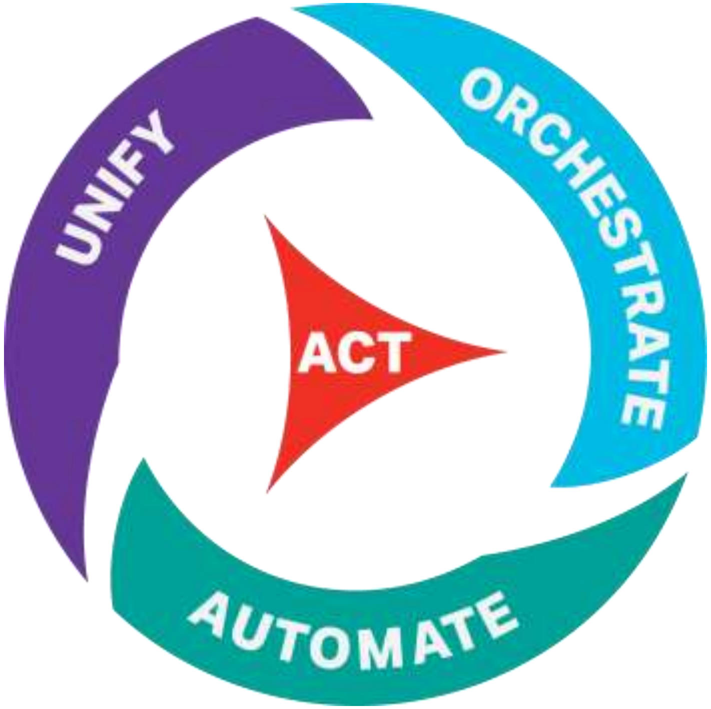
Automated Threat Response

csg INVOTAS

The Answer to Your Biggest Problem – Response Time.

An **Automated Threat Response** framework is composed of 3 steps to accelerate your response:

1. **Unify your security tools**
2. **Orchestrate your environment**
3. **Automate sensibly**



Security Automation

Full Automation

- Full Automation is hard coded rules in a system
- The more logic capabilities are in a system, the closer it is to artificial intelligence (ex. Boolean, if/then)
- Artificial Intelligence is a machine’s ability to make decisions.
- Current Artificial Intelligence capabilities are very immature

Security Automation

Practitioners’ views of Security Automation

- Does not belong in security
- Leaves the organization blind to security changes
- Requires trust in machine decisioning
- Is predictable, and can therefore be used against you

  (Consider - How is this different from you current approach?)

  – Self imposed Denial of Service Attack (versus DDoS)
- Prone to thrashing

Security Automation

Good Automation and Bad Automation

- When asked about Security Automation most practitioners are against it – It's bad!
- Allow systems to make machine speed DECSIONS – It's Bad!
- When asked about Automation for Decision Support and Repetitive Task completion, Low Risk items, practitioners are in favor of it – It's Good!
- Add Decision Support to Repetitive Task Completion with an analyst in the middle (removes the hard coding) – It's Good!

  (Hint: If the analyst is in the middle he is orchestrating)

Orchestration

Orchestration versus Automation

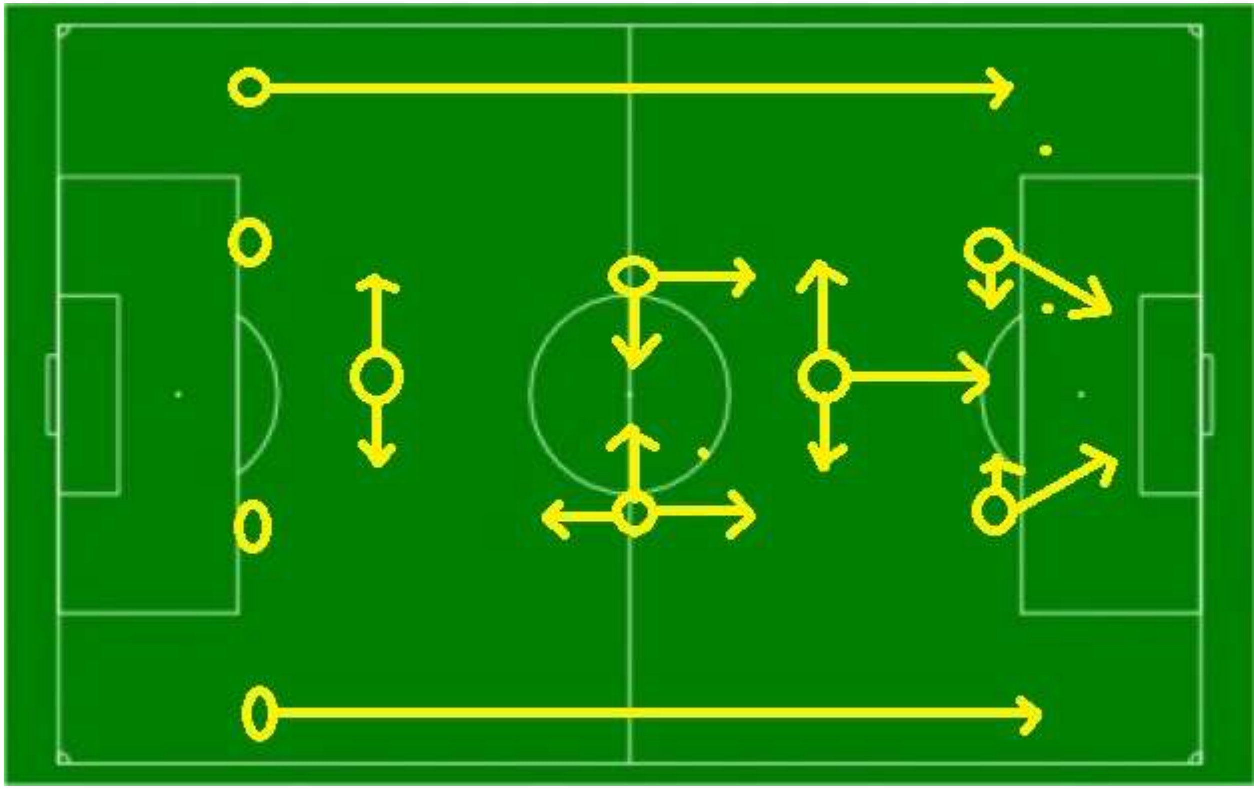
- **Full Security Automation**
  - – Hard coded full processes from start to finish
  - – Machine Decisioning & Execution
- **Orchestrated Automation (Orchestration)**
  - – Hard coded process modules
    - Decision Support (Enrichment & Guidance)
    - Decision Execution
  - – Human guided execution & sequence
  - – Supports Hybrid Full/Orchestrated responses
    - Buys time (shields up)
    - Provides Decision Support
- *Orchestration breaks up automated steps and places these action blocks into a library at the fingertips of the operator, to be triggered and sequenced on the fly. It keeps human intelligence and oversight in the action loop*

Orchestration or Automation – at the core

A football coach has a Command and Control console

He uses it to

- Direct his team’s movement
- Concentrate defenders on specific zones and players

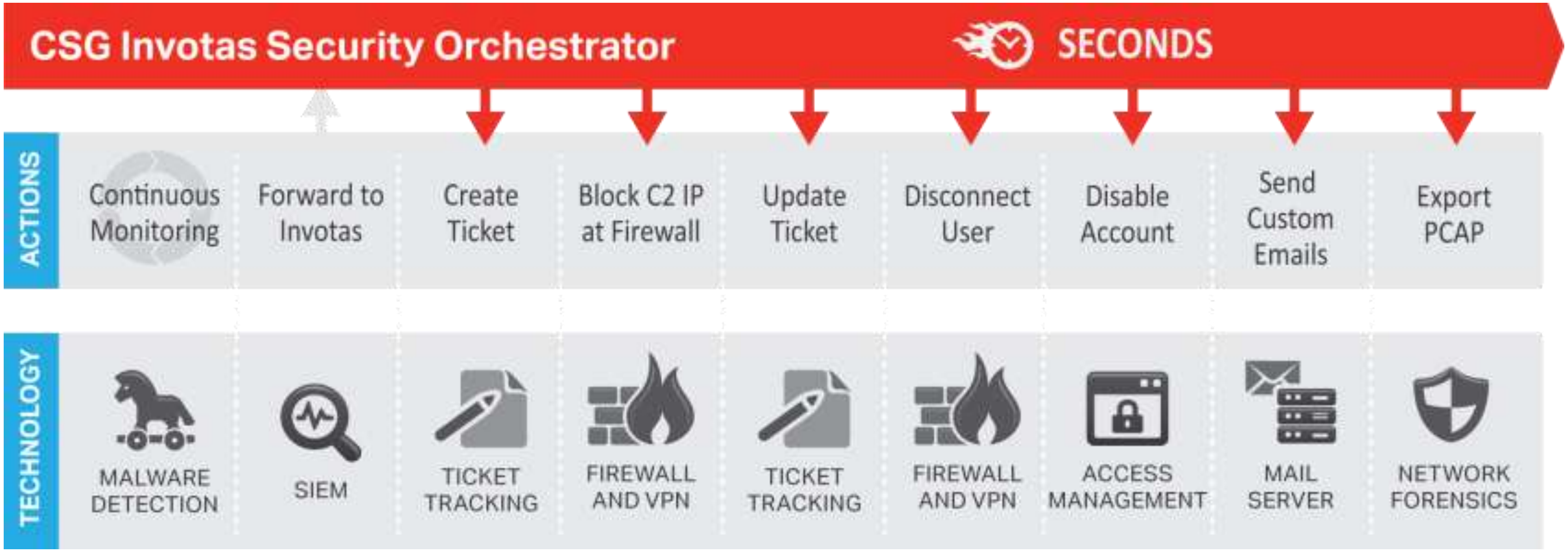


Is he

- Automating his team’s actions
- Orchestrating his team’s actions

Orchestrate Your Response

The automation of this workflow reduced the performance time of this process from 48 minutes to under 1 minute



CSG Invotas Security Orchestrator SECONDS

ACTIONS	Continuous Monitoring	Forward to Invotas	Create Ticket	Block C2 IP at Firewall	Update Ticket	Disconnect User	Disable Account	Send Custom Emails	Export PCAP
TECHNOLOGY	MALWARE DETECTION	SIEM	TICKET TRACKING	FIREWALL AND VPN	TICKET TRACKING	FIREWALL AND VPN	ACCESS MANAGEMENT	MAIL SERVER	NETWORK FORENSICS

Corrupted VPN Response Example

How to Build Orchestration

Understand your technical environment

- Conduct an Inventory of tools
- Clearly identify who owns those tools

Understand your governance environment

- Who is in charge in the event of an attack?
- Who is responsible for operations

Look for SIMPLE

- Look to create simplicity NOT complexity