

RSA[®]Conference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect **to**
Protect

SESSION ID: EXP-F03

Codifying the Brain: Automation, Alerts and a Human Resource Answer

Grady Summers

Chief Technology Officer
FireEye, Inc
@GradyS



#RSAC

The talent crunch

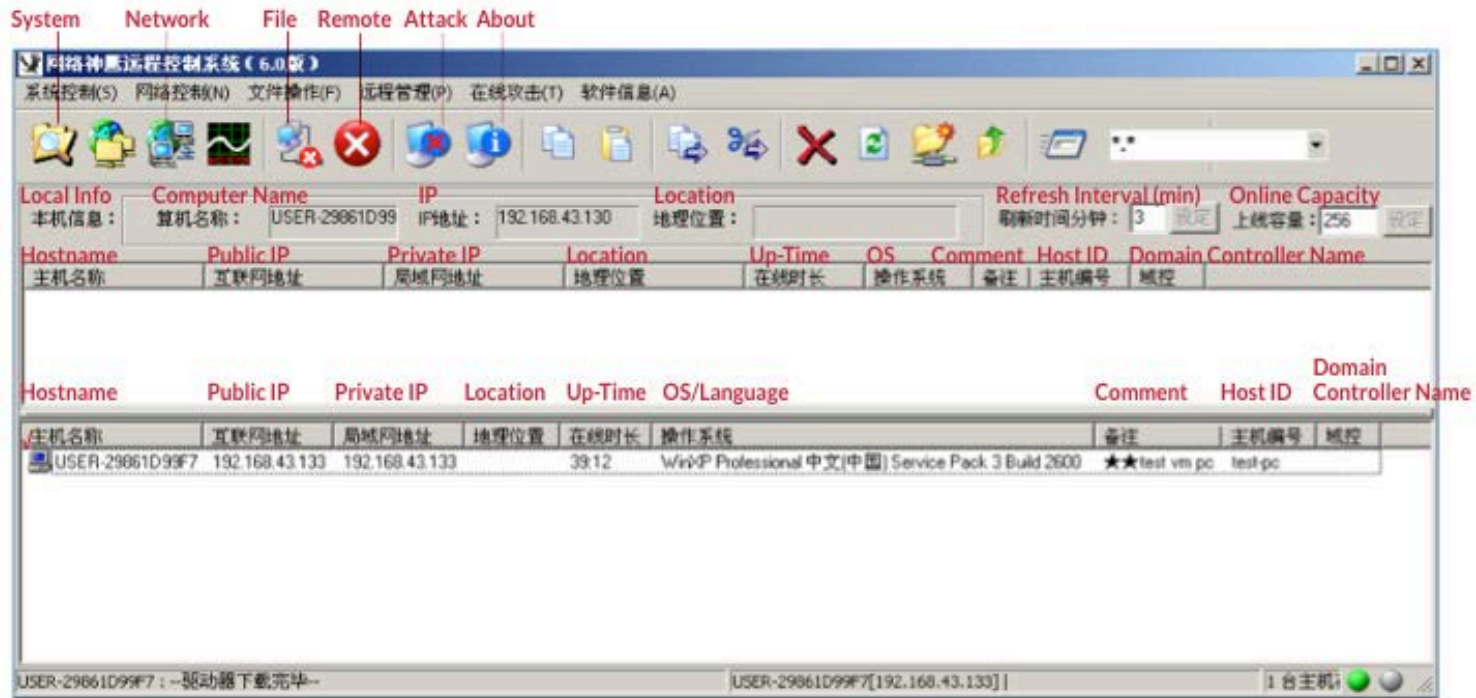


#RSAC

We have a shortage of good security talent—especially with the more specialized skills of incident response and hunting.

Where do we see automation today?

#RSAC



What if expertise could be codified?



#RSAC



What it means for IR



What it means for IR



#RSAC

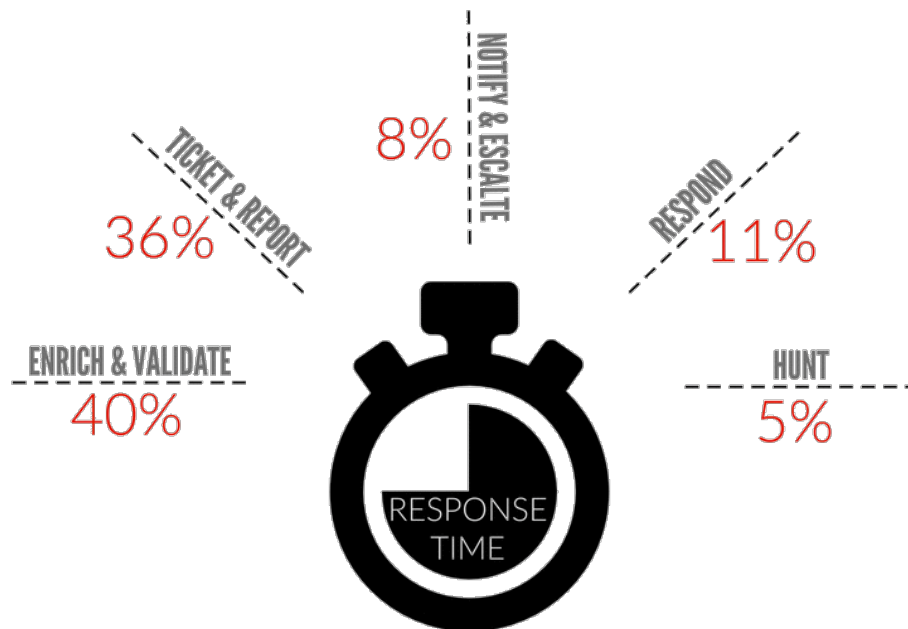
Of all alerts generated in the enterprise, 19 percent (3,218) are considered reliable but only 4 percent (705) are investigated.

Source: The Cost of Malware Containment <http://www.ponemon.org/blog/the-cost-of-malware-containment>

Where is time wasted?



#RSAC



What is automation/orchestration?



- Orchestration is the arrangement and coordination of a process
 - Orchestration is not necessarily automation
 - A well-orchestrated process could require human approval at each step
- Automation is the operation of a process with minimal human intervention
 - Automation is not necessarily orchestration
 - Simple steps of a process could be orchestrated (e.g., reverse DNS lookup) with minimal orchestration

What can be automated in an IR process?



#RSAC

Context

- Lookups against VirusTotal
- Lookups against AV
- Obtain domain registration history
- Look up the department of a user
- Look up the owner of an asset
- Query intelligence service for prior evidence
- Search SIEM for prior evidence
- Search endpoints for evidence of compromise

Containment

- Quarantine a host with endpoint detection/remediation software
- Block C2 at the proxy
- Update whitelisting software

Workflow

- Open a ticket in your case management system
- Send emails to impacted users
- Automatically forward/escalate based on automated decisions
- Etc...



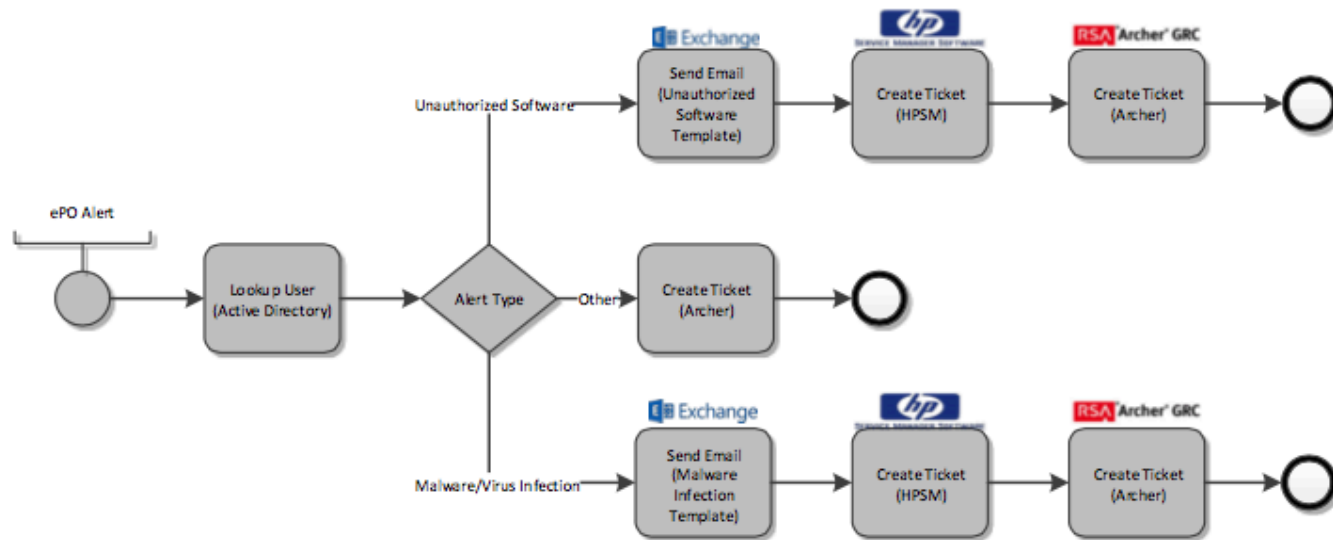
Real-World Use Cases



Antivirus Alert



#RSAC

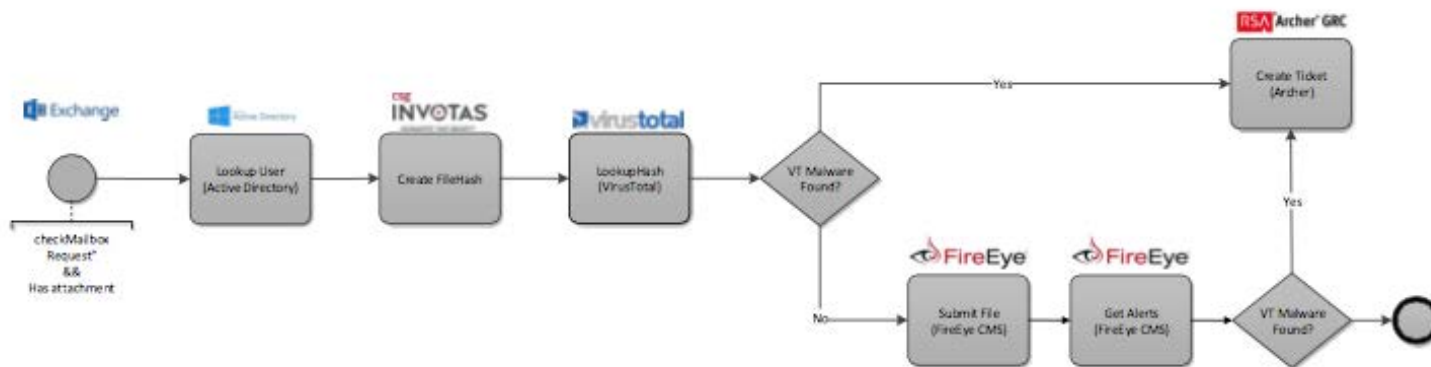


1,200 hours per year → 40% time savings = 2,288 hours/year saved

Suspect email analysis



#RSAC

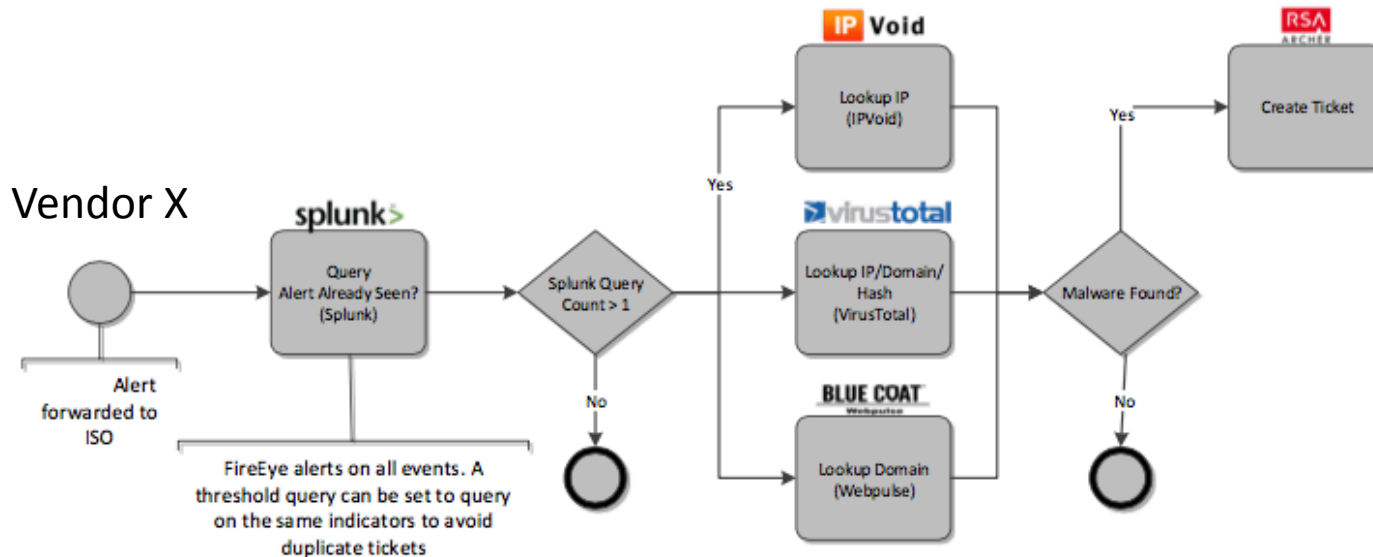


8,800 hours per year → 65% time savings = 5,720hours/year saved

Advanced Threat Alert



#RSAC



3,520 hours per year → 65% time savings = 2,288 hours/year saved



Challenges and Best Practices for Automation



Challenges



- What about the dark arts of incident response?
- What about ambiguity?
- Should code really be making decisions?
- What if automation reaches the wrong conclusion?
- This is my job!

“Lean Before Digitize”



- Automating ineffective processes just results in faster ineffectiveness
- Consider adding new sources that were previously omitted due to time constraints

Understand your metrics and targets



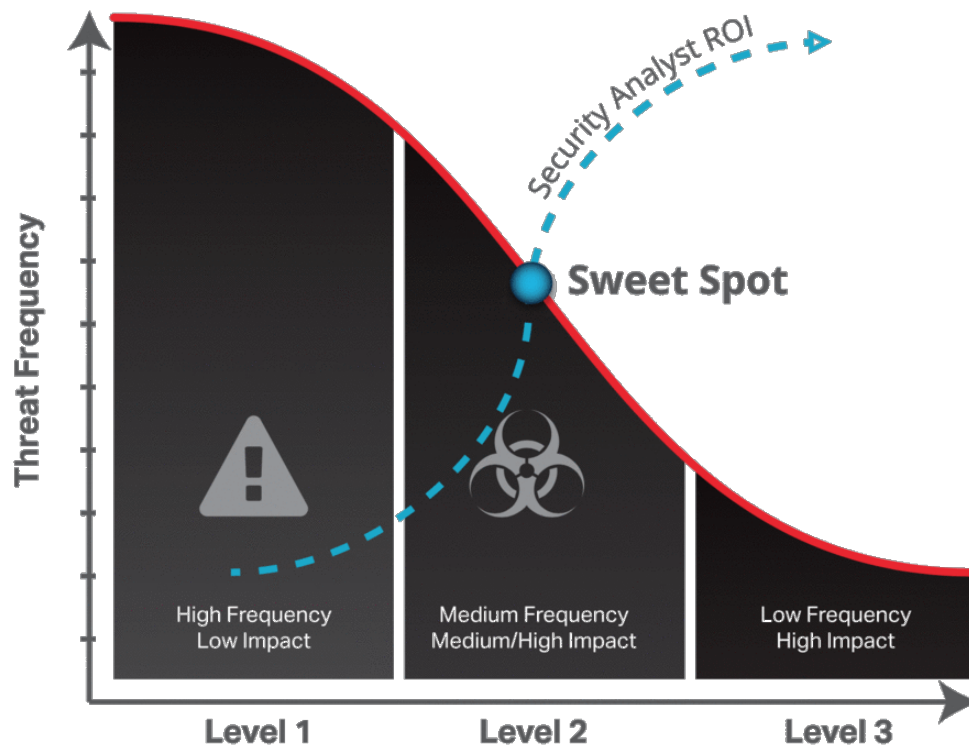
#RSAC

- Time to identify (TTI)
 - Fast incident identification is a hard requirement for the decision making and response process
- Time to respond (TTR)
 - TTR is crucial to early interruption of threats
- Frequency
 - The average number of incidents over a given time window
- Risk-Regret
 - High risk-regret actions directly affect ROI as these are likely to remain as human initiated – whereas low risk-regret are excellent candidates for full automation
- Integration readiness
 - Readiness for integration can be impacted by several factors including technology or process limitations. Integration readiness will evolve over time with improvements in both.

Automate the right types of incidents



#RSAC



Deploy carefully



#RSAC

- Selectively identify the processes and activities with the most return from an analyst time and effort point of view.
- Automate your actions as close to the threat window as possible. Reduce your threat exposure by blending human and machine actions for the best (and fastest) results.
- Measure your successes – refine and improve them.
- Create new courses of action as you master existing playbooks.
- Reuse everything.
- Control the excitement.
 - Teams often want to jump in and create playbooks, which is great. But this can lead to confusion.
 - Instead, create a priority-based list with an initial team, then identify the growth process.

Define and communicate the win

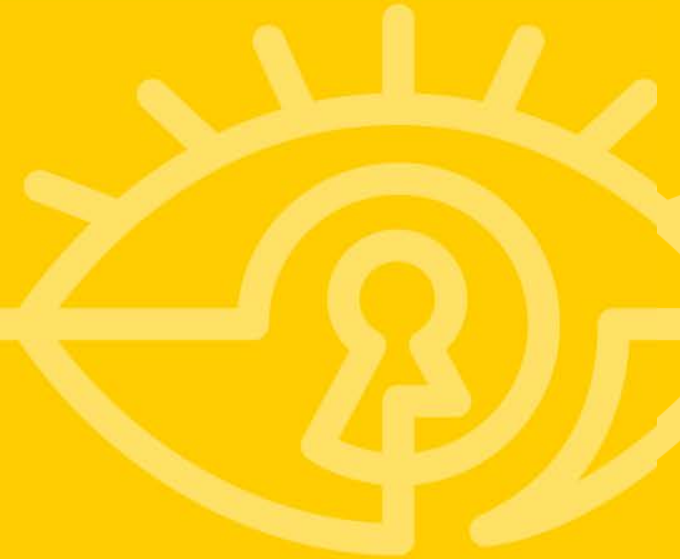


Why are you automating?

- To reach a cost-out target?
- For the elimination of annoying tasks?
- So that your team can devote more time to hunting?



Applying Automation



Getting started with automation



- Next week you should:
 - Identify low-value / high-frequency tasks within your IR process
- In the first three months following this presentation you should:
 - Automate these processes
 - Start scripting; graduate to commercial tools when connectors and playbook libraries become your bottleneck
- Within six months you should:
 - Have your analysts start hunting with all of their free time!