The Role of Orchestration in Incident Response

Ted Julian, VP Product Management

IBM Resilient

Agenda

- The IR imperative
- Automation hype vs. reality
- Orchestration and automation
- IR maturity model
- Use cases
- Conclusions

resilient

The Incident Response Imperative

Most organizations are unprepared to respond to cyberattacks:

- 73% of French respondents and 71% in the UK are not confident in their organisation's ability to recover from cyberattack.
- However, only 55% in Germany are not confident. The global average is 66%.
- Globally, 70% spend the same or more time resolving a cyber incident than a year ago.

"Insufficient planning and preparedness," "complexity of business and IT processes," and "insufficient risk awareness" are the biggest barriers to cyber resilience:

- In Germany, the top barrier is "complexity of business processes" (66%).
- In France and the UK, the top barrier is "insufficient planning and preparation" (68% and 73%, respectively).

Most organizations do not have a proper cyber security incident response plan (CSIRP) in place:

- Globally, 75% do not have a CSIRP in place and applied consistently across the organization (74% in the UK and 77% in France).
- In Germany, 34% have a CSIRP in place and applied consistently across the organization.

An incident response platform can improve cyber resilience:

- Of those who said their cyber resilience had improved in the last 12 months, 61% in Germany, 55% in the UK, and 58% in France said an incident response platform was among the most effective security technologies for improving cyber resilience.

Automation Hype

- Your alerts go away
- Your issues automatically resolve
- Your team becomes super human

What's not to like?

Automation Reality

What would you automate?

- 70% don’t have a plan

Why would you automate it?

- Most don’t know what their top issues are

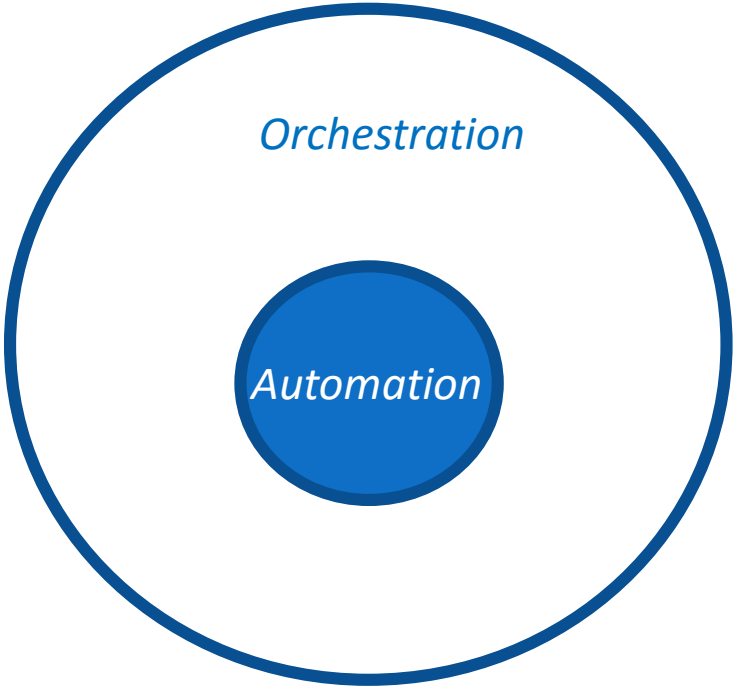
Is it automate-able?

- False positives can make the “cure” worse than the disease
- Escalations? Exceptions?
- Can you really pull humans out of the equation?

How would you know if you succeeded?

- Most can’t measure their response time

Orchestration and Automation



Orchestration

Humans set it up and guide computer execution.

resilient

Am I Ready?

How Should I Start?

Incident Response Maturity Model

Maturity Level		Ad-hoc		Mature		Strategic
		As Needed	Dedicated Part-Time	Full-Time	SOC/IR+	Fusion
Existing IR Capability	People	• 0-1	• 1-3 • Specialization	• 2-5 • Formal roles	• ~10 • Shifts (possible 24x7)	• 15+ • Intel, SOC, and IR Teams
	Process	• Chaotic and relying on individual heroics • Reactive • General purpose run-book • Tribal knowledge	• Situational run books • Some consistency • Email-based processes	• Requirements and Workflows documented as SOPs • Some improvement over time	• Process measured via metrics • Minimal threat sharing • Shift turnover • SLAs	• Processes continually improved and optimized • Threat sharing • Hunt teams
	Technology	• A-V • Firewalls • IDS/IPS	• SIEM • Sandboxing	• Continuous Monitoring • Endpoint Forensics • Tactical Intelligence	• Malware Analysis • Additional Intelligence • IT Operations Integration	• Intel+IR Drives Security Program • Strategic Intelligence • Coordination with Physical Security/Intelligence
CMM* Equivalent		Initial	Repeatable	Defined	Managed	Optimized

Source: Ted Julian, IBM Resilient; Sean Mason, Cisco
*CMM = Capability Maturity Model

Progressive Orchestration

Crawl

- Define and refine SOPs
- Define KPIs and measure
- Identify opportunities for orchestration

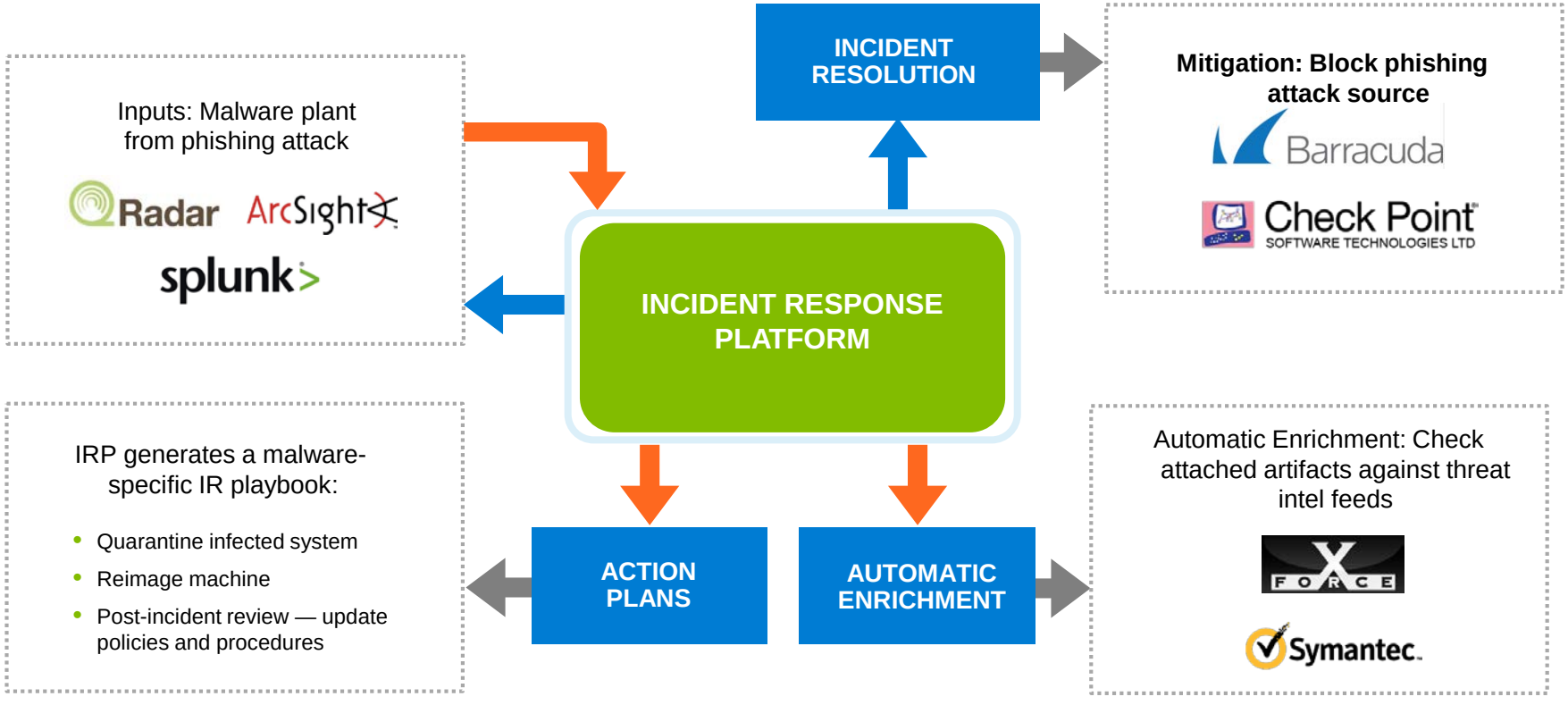
Walk

- Test orchestration of identified opportunities
- Refine based on experience
- Refine KPIs and measure

Run

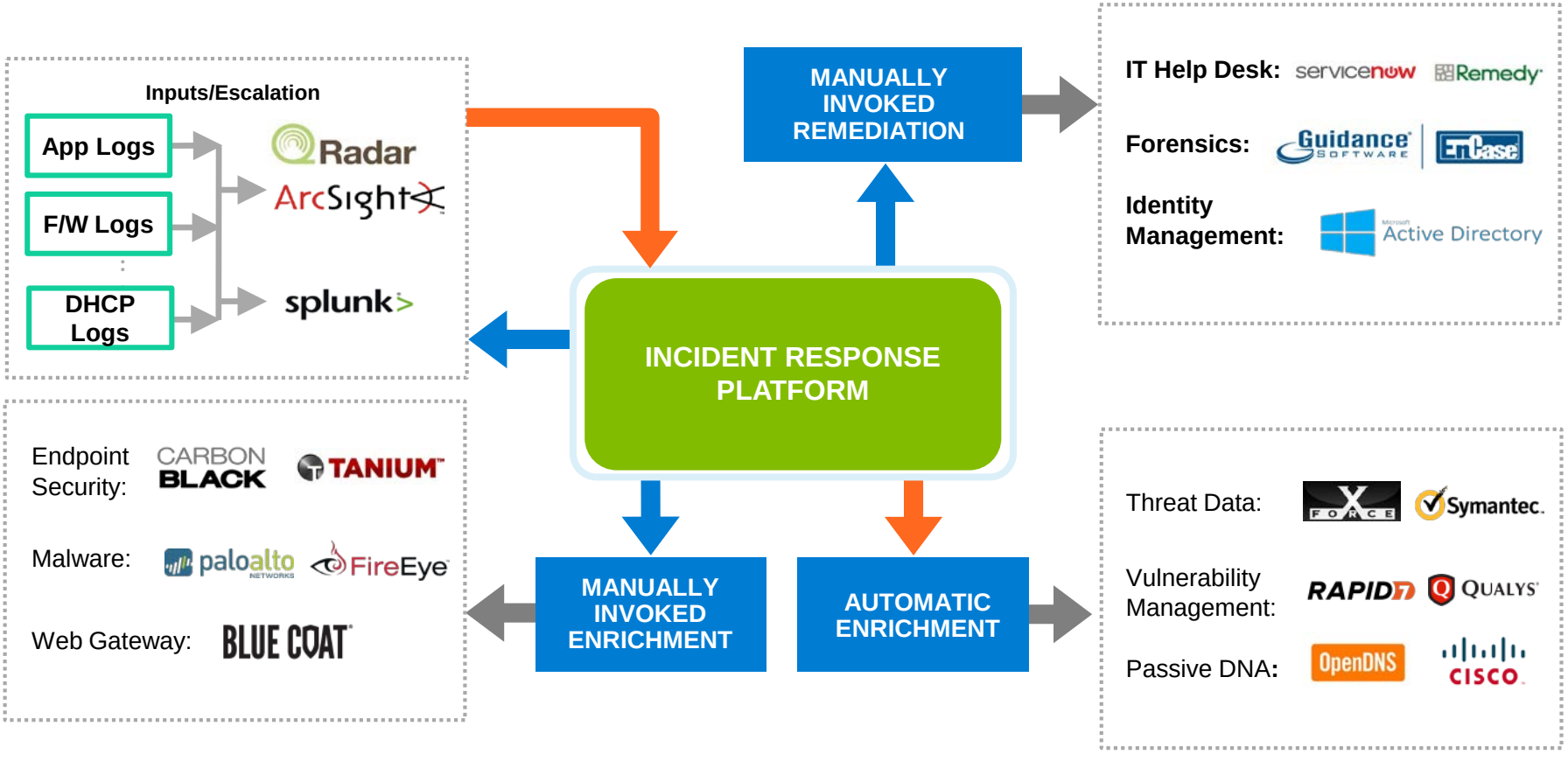
- Automate proven processes
- Refine approach for continuous improvement
- Identify next wave of orchestration opportunities

Use Case: Malware Outbreak – Maturing

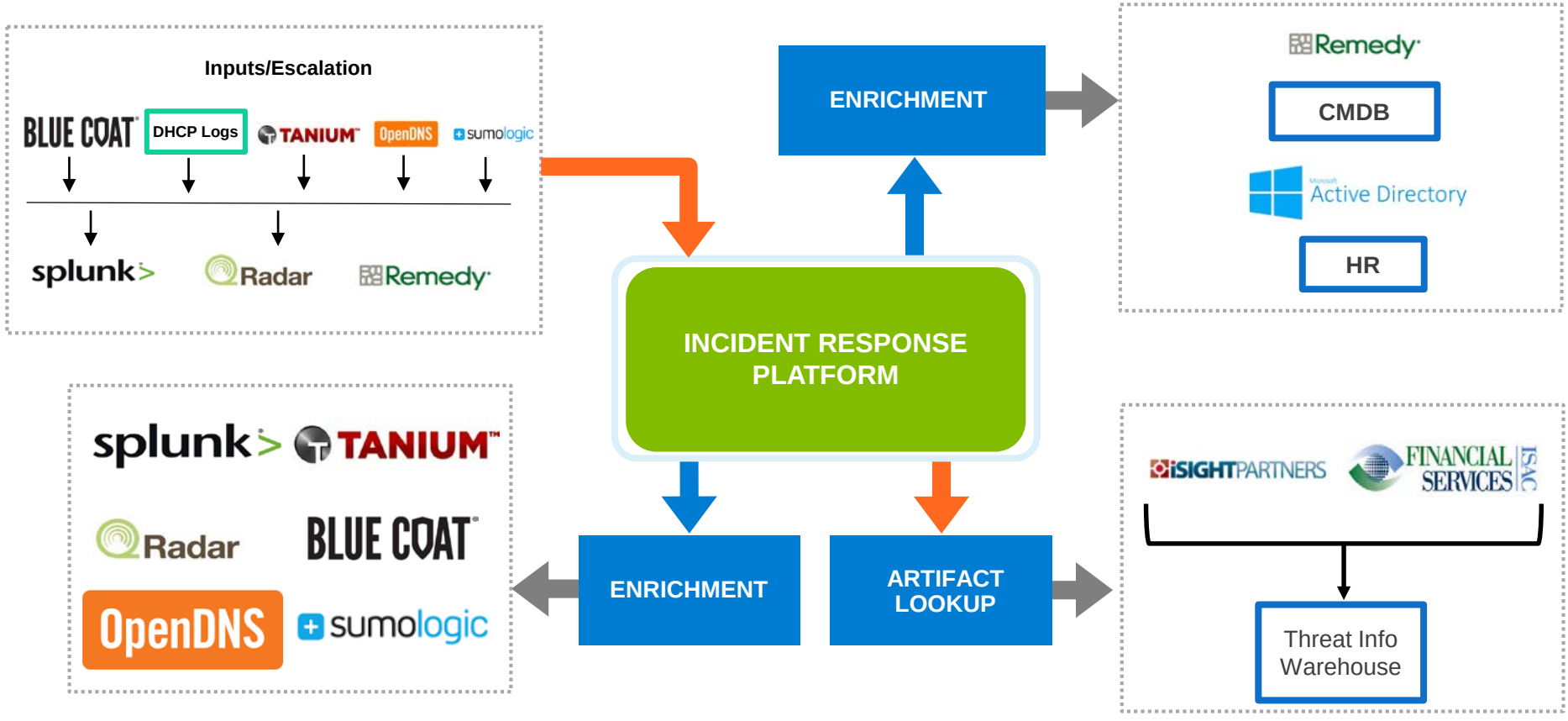


resilient

Use Case: Enterprise Fusion Center



Use Case: F50 customer in financial services



Conclusions

- Orchestration is the goal – automation is one piece
- Leverage the maturity model to baseline where you are at, and where and when to begin
- Crawl, walk, run
- Use metrics and KPIs to define orchestration candidates and measure success

Questions?