

# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-W03

## HOW TO: Aggressive Remediation In An APT World

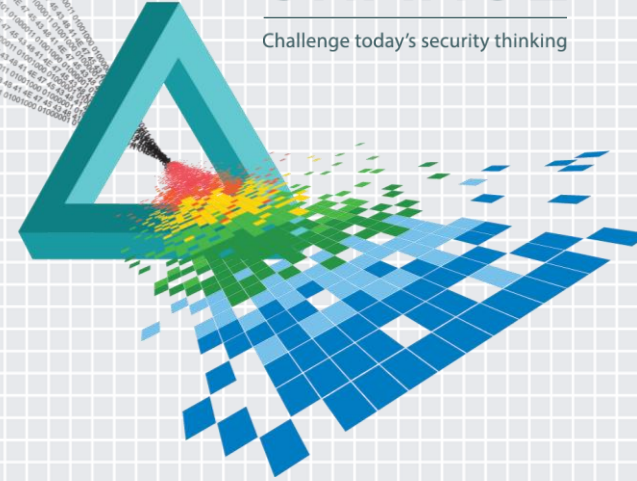
**Jim Jaeger**

---

Chief Cyber Services Strategist  
Fidelis Cyber Security  
@jimjaeger3

# CHANGE

Challenge today's security thinking



# Why Aggressive Remediation?

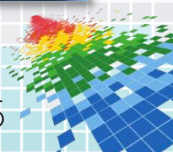


SCENARIO

Repeated breaches by the same advanced attackers

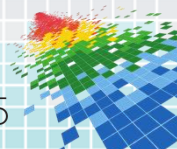
OR

A breach that has gone undetected for weeks or months



# HOW TO: Aggressive Remediation

- ◆ Traditional IR models versus Advanced Attack models
- ◆ What is eradication?
- ◆ The two eradication models
  - Sequential eradication
  - Event-focused eradication
- ◆ How do you chose which model to employ
- ◆ Considerations for success!

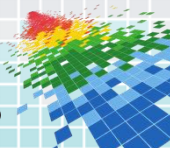


# Incident Response (IR) Models

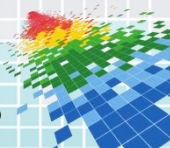
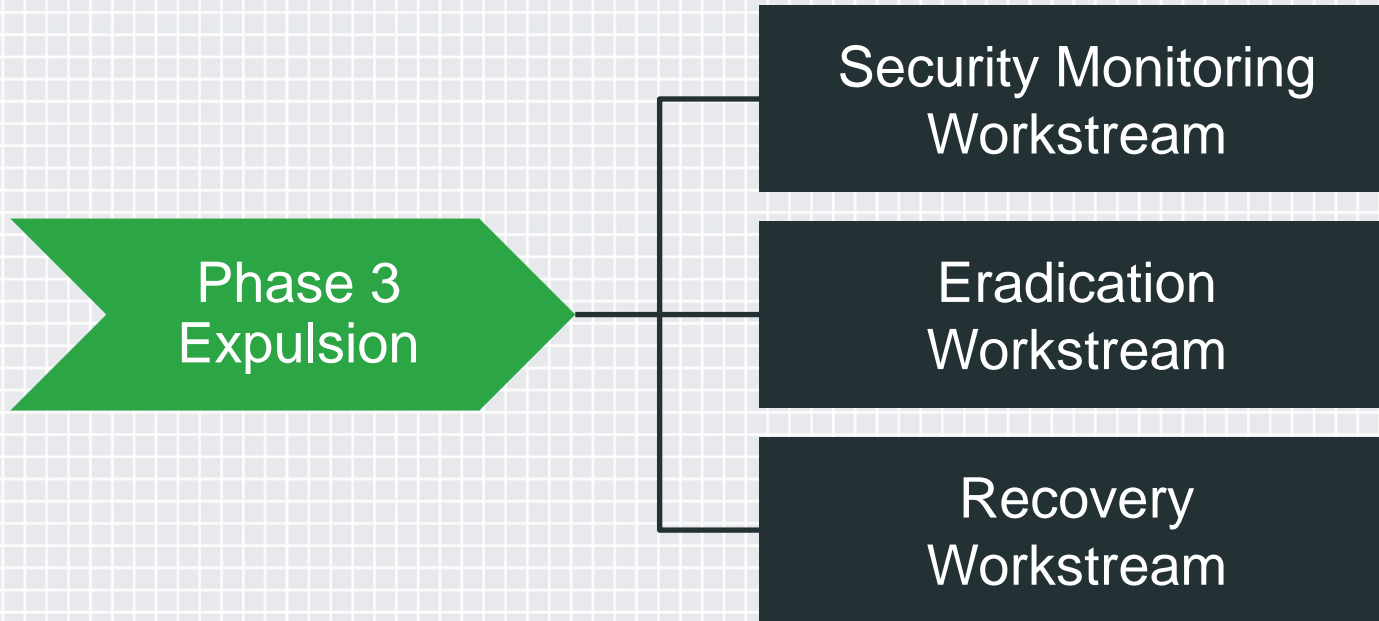
## Traditional IR



## Advance Attack IR

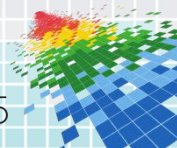


# Expulsion Activities



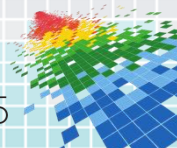
# Eradication

# What is eradication?



# Eradication

## What are the two approaches to eradication?



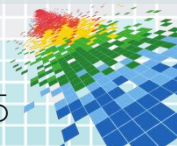
# Sequential Eradication



- + Attackers tools are eliminated quickly
- + Risk of loss/damage may be lower
- + Cost is lower



- Loss of critical data on attacker tactics
- Attackers may go quiet making it more difficult to find their tools
- Investigative resources may be shifted to eradication
- Risks retaliatory damage




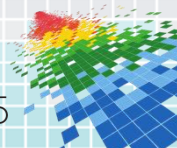


# Event-focused Eradication



- + Better understanding of attackers tools, tactics, targets and motivations
- + Minimizes retaliatory risk

- 
- Requires extensive planning and sophisticated execution
  - Requires sophisticated approaches to reduce data loss
  - Cost is usually higher



# Considerations for Choosing Approach

Organization's risk tolerance

Depth and breadth of entrenchment

Confidence in containment approach

Ability to lock down active directory (AD)

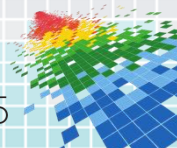


Network security monitoring capabilities

Ability to scan for attacker's tools

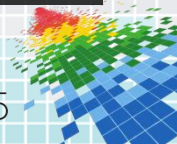
Ability to validate removal of attacker's tools

Sufficient staff & expertise to plan and manage complex execution



# HOW TO: Tips for Success

- ▶ Detailed planning
- ▶ Prep and stage resources
- ▶ Communicate with law enforcement and other partners
- ▶ Ensure robust network security monitoring is in-place
- ▶ Develop eradication scripts and test them in lab
- ▶ Scan, scan and rescan to validate removal of attacker's tools
- ▶ Sufficient staff & expertise to plan and manage complex execution



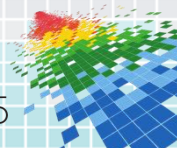
# HOW TO: Don't Be A Repeat Victim!



Add an eradication step to your IR plan

Train and exercise for eradication

Engage IR SMEs to guide your effort



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Questions?

**Jim Jaeger**

+1 443-926-1159

[jim.jaeger@fidelissecurity.com](mailto:jim.jaeger@fidelissecurity.com)

Twitter: [@jimjaeger3](https://twitter.com/jimjaeger3)

