Set Solutions, Inc.

Incident Response

Things I Wish I Had Known The First Time

Who Is Set Solutions, Inc.?

- 20+ years in IT Security
- Full range of compliance, security and network services
- Relentless research
- Vendor agnostic
- We help safeguard several of the largest companies in the world
- Very happy customers!

Who Am I?

- Not this guy…
- Senior Engineer with Set Solutions, Inc.
- 18 years in IT Security, IT, and IT Audit
- Security experience in University, Healthcare, Aerospace/Defense/Industrial industries…

Set Solutions, Inc.

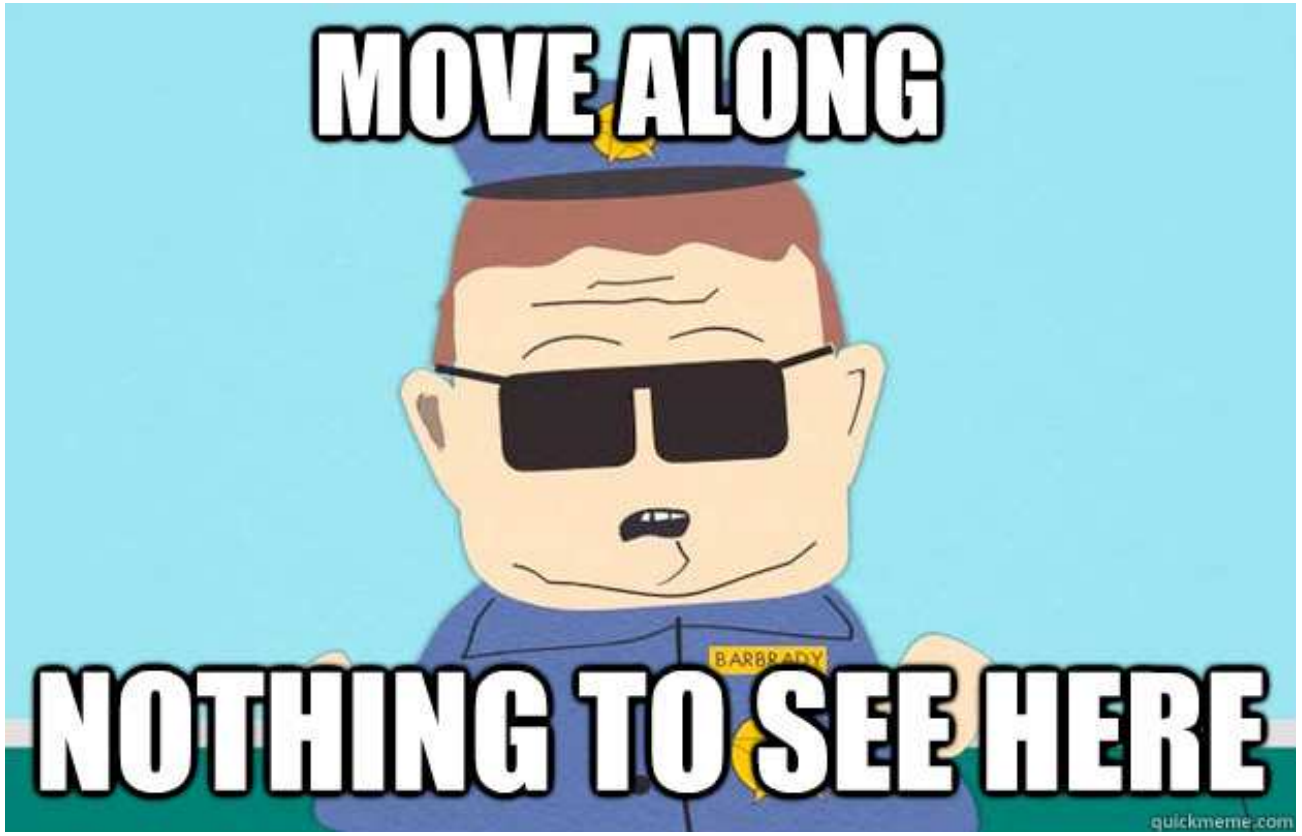
What Is This About?

- Things I wish I knew before this happened

Set Solutions, Inc.

What Are Your Goals?

- Clean up as quickly as possible and move on.



Set Solutions, Inc.

What Are Your Goals?

- Identify…
  - TTP's
  - Systems affected
  - What controls failed?
- Minimize loss of data or other damages
- Remove the threat
- Secure the environment
- Get back to normal operations
- LEARN FROM EXPERIENCE!

Set Solutions, Inc.

You Need A Plan

Set Solutions, Inc.

Example IR Plan

- Overview / IR Policy
- Roles and Responsibilities / Incident Response Team(s)
- Incidents Requiring Action
- Procedures for Response Steps:
  - Identification
  - Containment
  - Eradication
  - Recovery
- Call List / Communications
- Current Network Infrastructure Documentation
- Existing Security Controls Documentation/Procedures
- Retainer for experts
- SLAs with existing partners, vendors, etc.
- Training and Awareness
- Lessons Learned

Set Solutions, Inc.

IR Team Skills

- Technical
- Non-Technical

Set Solutions, Inc.

IR Team Members

- IR Team:
  - IT Security
  - IT - Networking, Server, Apps, AD, Desktop
  - Consultant(s)
  - Project Management
- Need an Executive Sponsor!

Set Solutions, Inc.

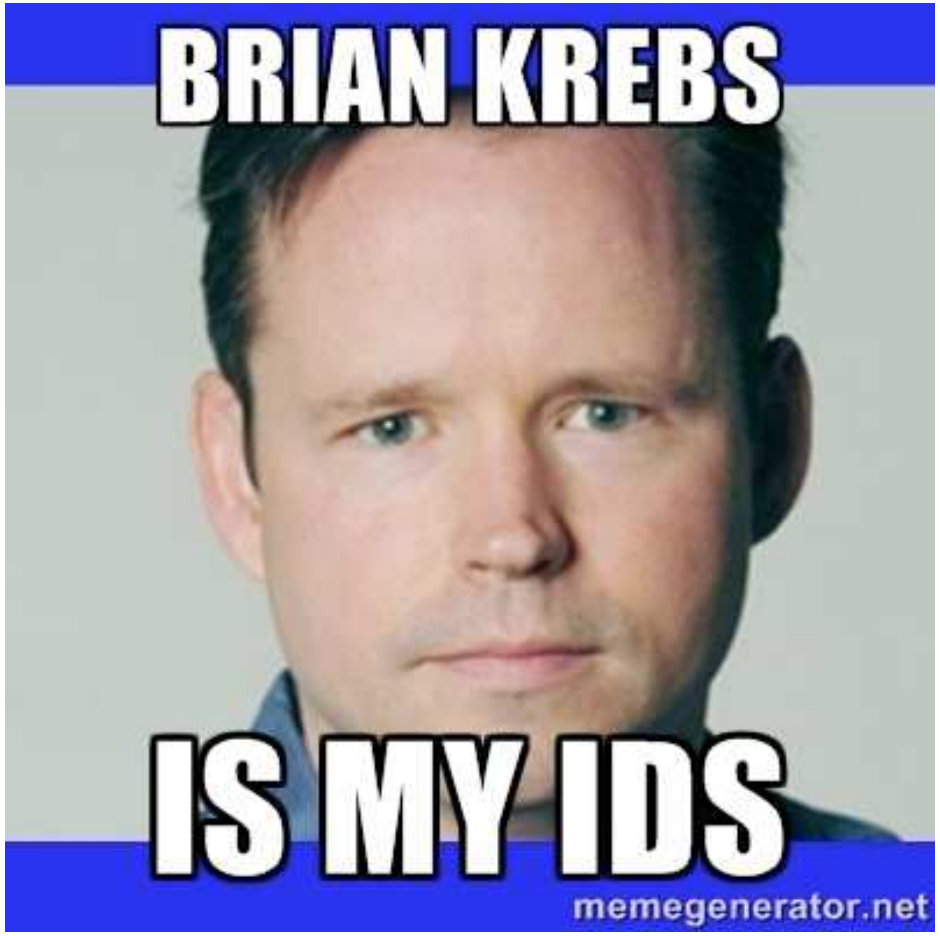
Other Groups to Keep in the Loop

- Other IT - HelpDesk, Desktop Support, Business Apps, Web Development
- 3rd Party IT Providers
- Compliance/Privacy
- Audit
- Legal
- HR
- Corporate Communications

Set Solutions, Inc.

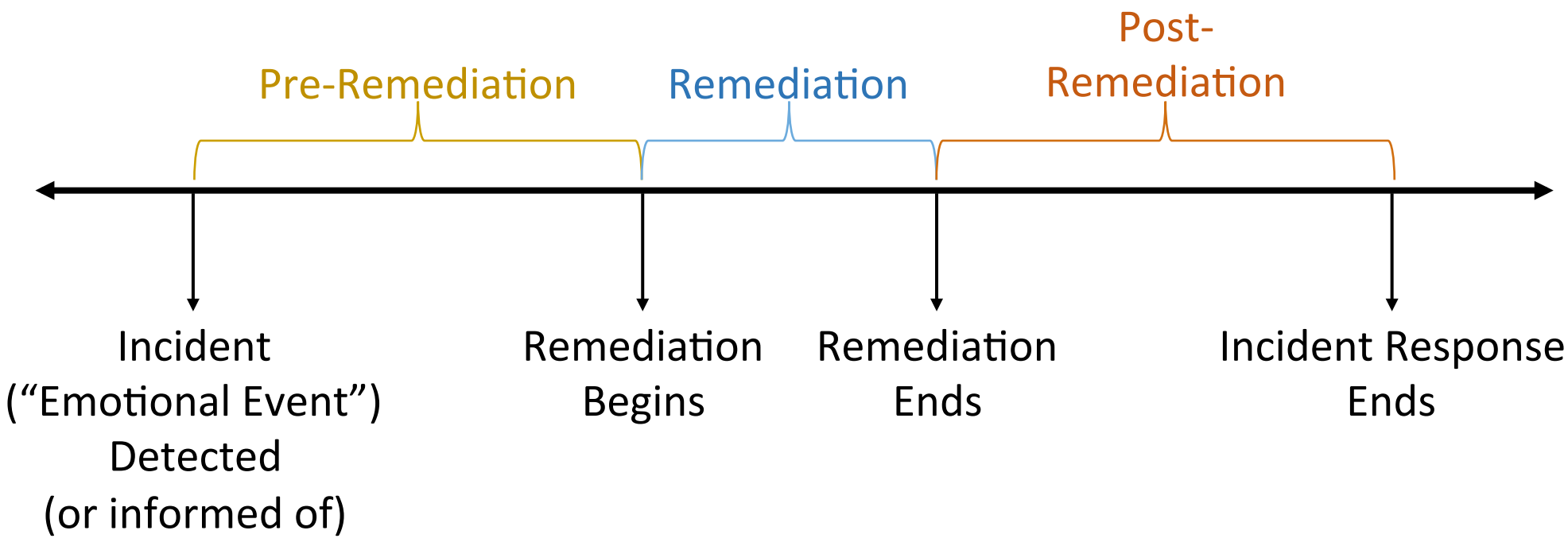
What Are Your Current Capabilities?

- What skills and tools do you have?
- What is your visibility? At perimeter and internal…
- Where are your privileged accounts? Do you know?
- Know what and where your gaps are…



Set Solutions, Inc.

Incident Response Timeline

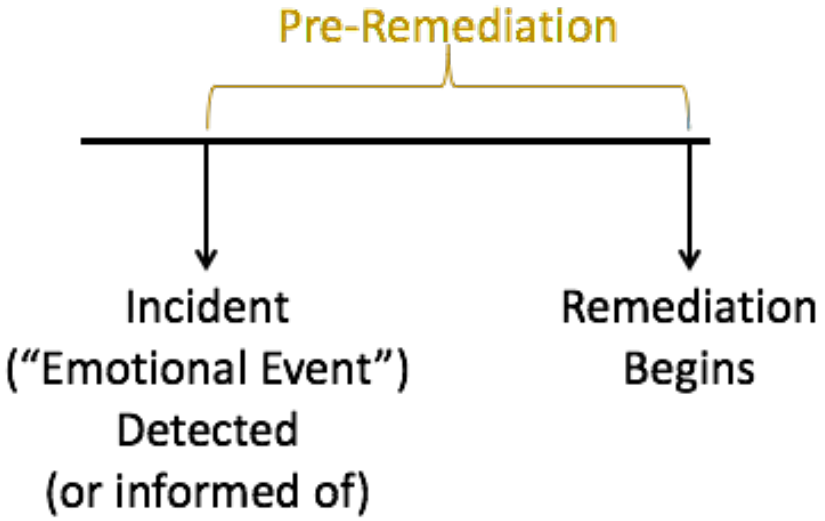


Set Solutions, Inc.

Incident Detected / “Emotional Event”

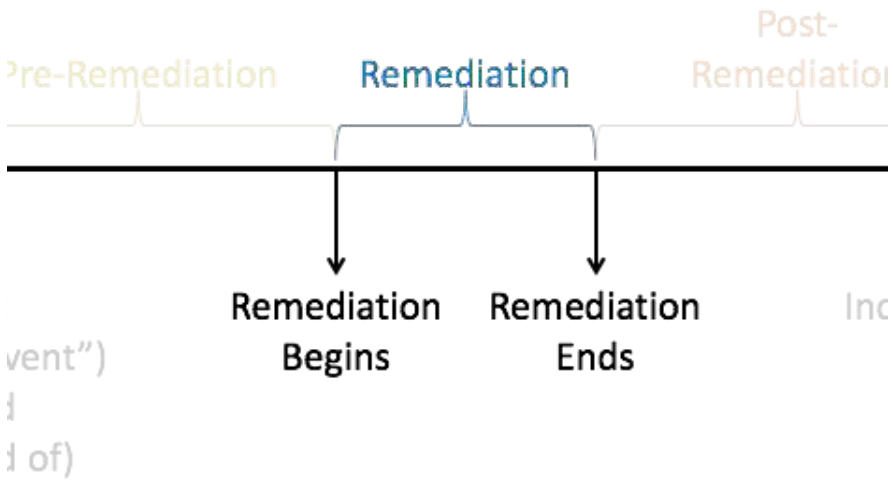
Pre-Remediation / Posturing Phase

- Fire up the IR Team and Processes
- Ramp up detection / monitoring / logging
- Control Lateral Movement
- Change Management
- SLAs / 3rd Party IT Providers



Set Solutions, Inc.

Remediation Phase

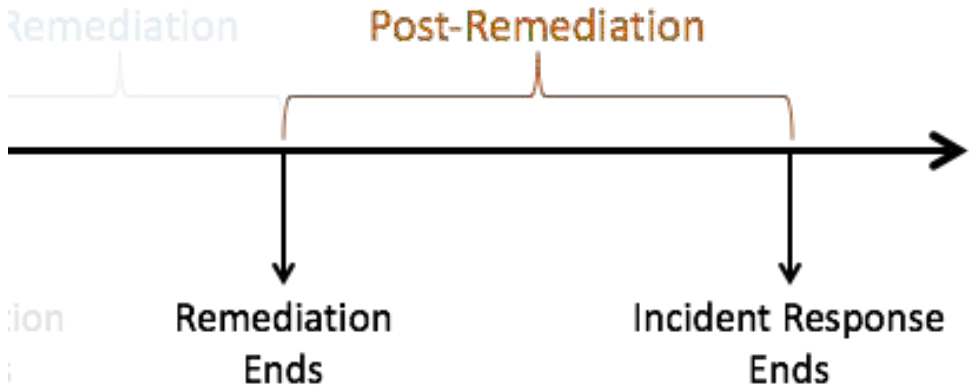


- Point in time when an organization has…
  - Identified the threats in their environment including relevant malicious domain names, IP addresses, and URLs
  - Compromised systems have been identified
  - Pre-remediation controls have been implemented
- Organization feels they are ready to remove the current threats
- Usually a weekend or after-hours event

Set Solutions, Inc.

Post-Remediation Phase

- Ensure malicious activity is not ongoing
- Make sure weaknesses have been mitigated
- Short-term and Long-term additional posturing…



Set Solutions, Inc.

Incident Response Ends

- Learn from it!
- What worked…what did not work?
- People, Processes, Tools…
- Vendors, Business Partners…
- Give kudos to members…

Set Solutions, Inc.

Set Solutions, Inc.