RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Restoring Trust After A Data Breach

SESSION ID: CDS-W08

Dwayne Melançon, CISA

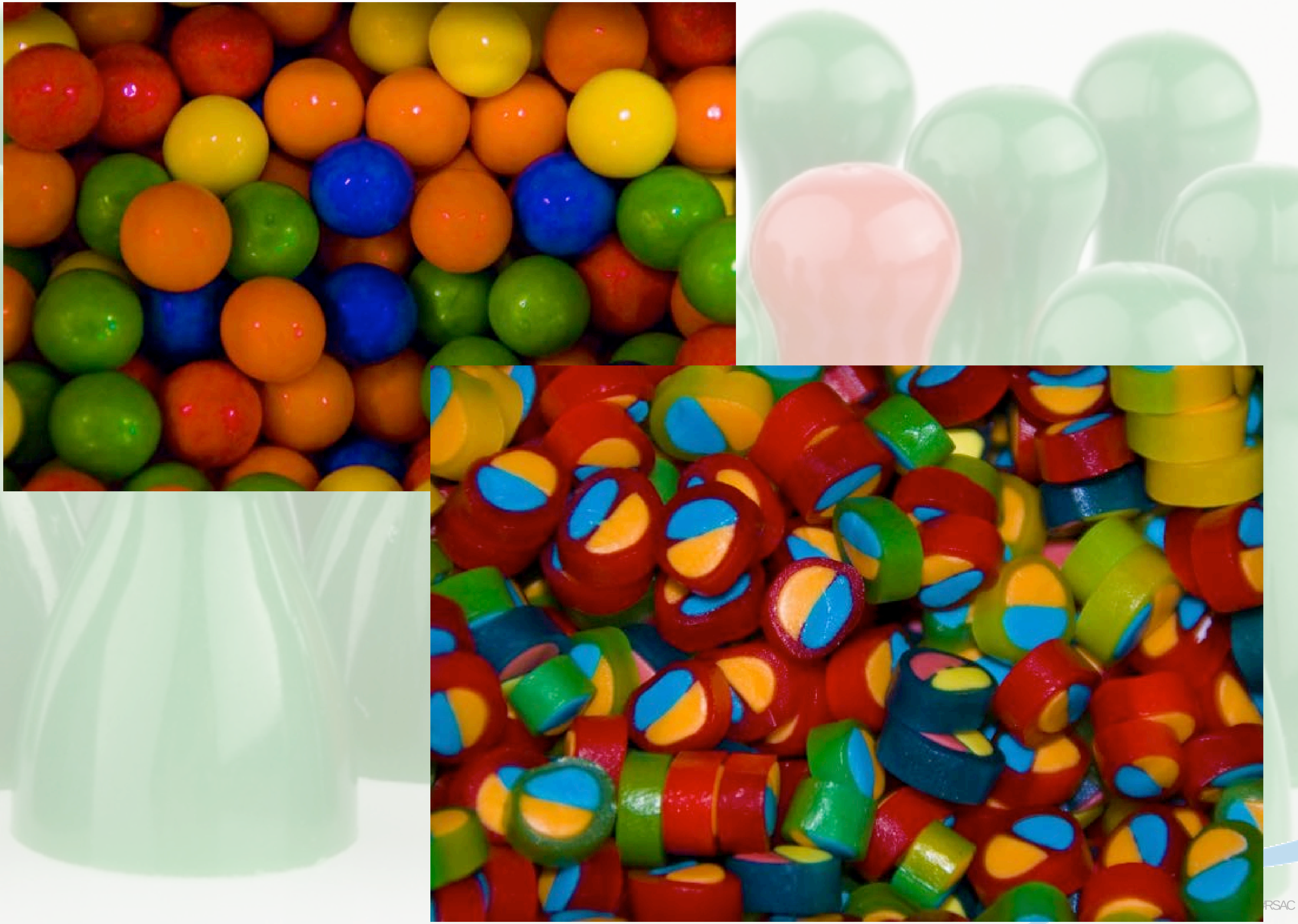
Chief Technology Officer
Tripwire, Inc.
@ThatDwayne

#RSAC

“It’s the not knowing that’s the worst…”

After A Breach, There Are More Questions Than Answers

- “What happened?”
- “What was done to compromise my systems or data?”
- “What’s the extent of the damage?”
- “Which systems can I trust?”
- “How quickly can I figure out where I stand?”
- “What did I lose?”
- “How do I keep this from happening again?



A Systematic Approach: Restoring Trust After A Breach

A More Detailed View

- Stabilize the patient
- Know what you have and prioritize by risk and value
- Harvest system state information from your production systems
- Compare what you have to what you deployed
- Remove suspect systems from the environment and return to a trustworthy state
- Continuously monitor and validate to prevent re-compromise
- Communicate in a way that builds trust and confidence

Stabilize The Patient

Reduce The Opportunity For Further Compromise… And Confusion

- Remove or reduce access to production
- Change all production credentials
- Freeze changes
  - Except with deliberate management review and scrutiny

- Don’t forget about 3rd parties!

Know What You Have - Prioritize By Risk & Value

You Can't Do Everything At Once – Set Priorities To Figure Out Where To Start

- You Can't Do Everything At Once
  - Inventory your environment to ensure you have a comprehensive view
  - Determine what's most important (and document your criteria)
    - Fragile artifacts
      - High business impairment cost
      - "Make or break" for your business
      - Big consequences
  - Assess your data sources and ensure they are protected
  - Stay on the same page as business management

Define What "Good" Looks Like

Establish A Trusted Reference Point

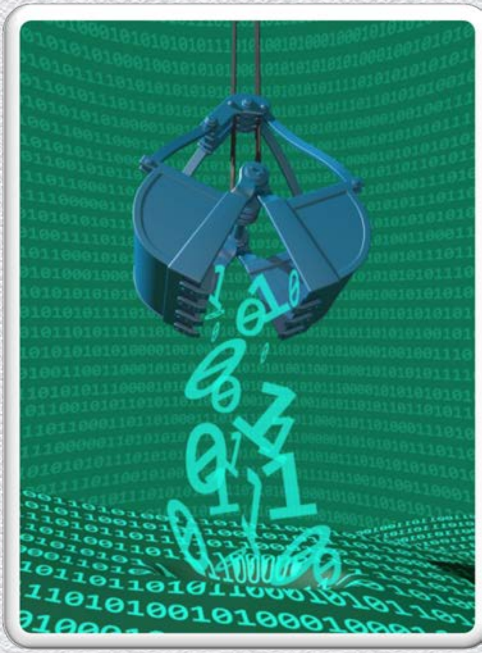
- Figure out what should have been deployed
  - Provisioning sources
  - System & application templates
  - Configuration standards
  - Pre-prod / test systems
    - Include servers, network devices, databases, accounts
  - VM libraries, definitive software libraries, deployment packages, etc.
  - Leverage redundant data centers
  - Restore from backup
  - Worst case, build reference infrastructure by hand

CERTIFIED

Harvest System State From Production

Assess The Current State Of Your Systems

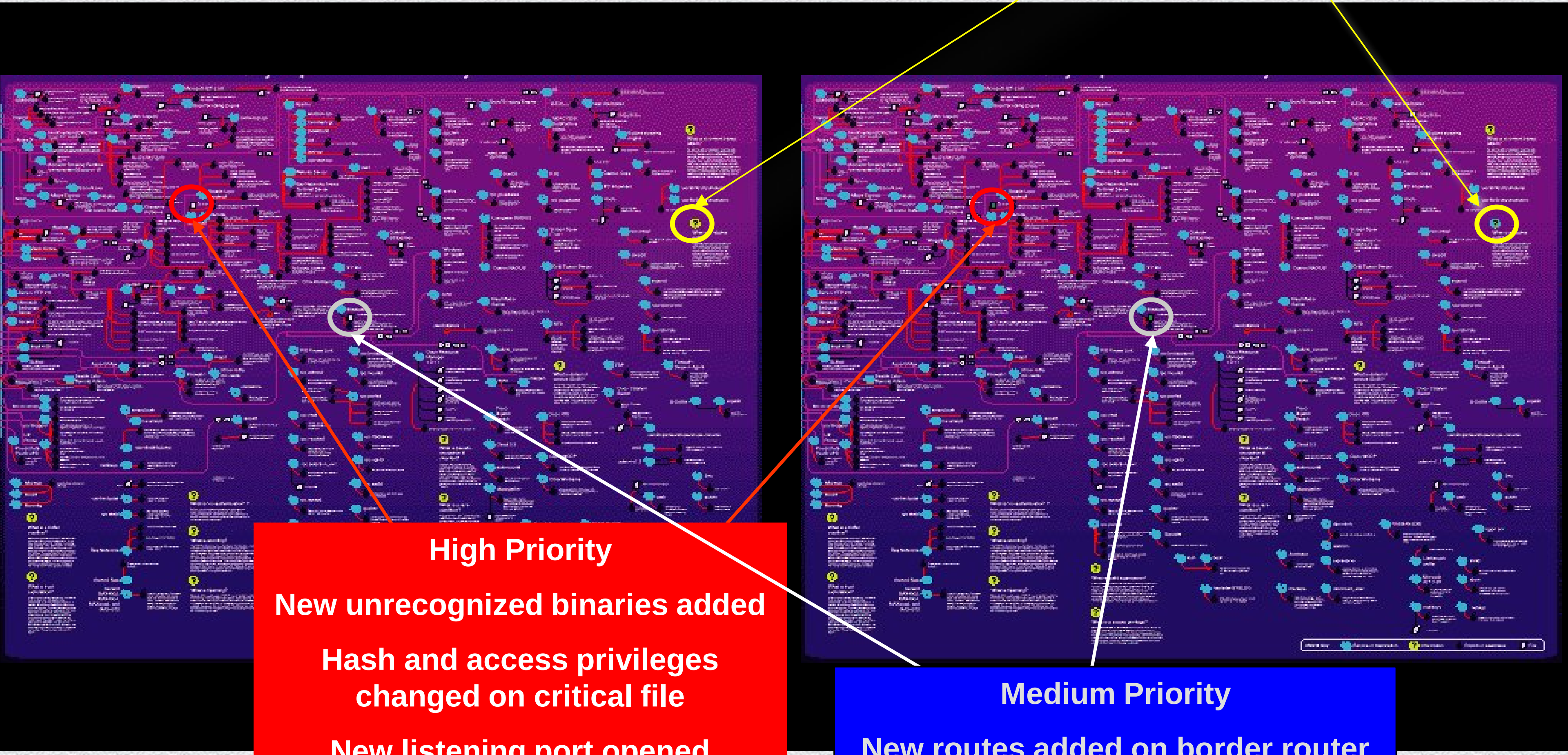
- Determine how you will harvest data
  - Agent, agentless, manual inspection, etc.
- Harvest OS, applications, settings (configs), user information, file hashes, etc.
- Move harvested data to a discrete storage location
  - Offline analysis, containment of investigation data, etc.



Compare What You *Actually* Have vs. What You *Should* Have

Figure Out What Is Different From What You Deployed

- Compare current state with what you expect
- Rank findings and difference based on risk and value
- Correlate system state information with other sources for greater accuracy
  - Flow and traffic data, log data, etc.
- Automation is your friend



Low Priority

Non-admin user added

Password policy varies from policy

High Priority

New unrecognized binaries added

Hash and access privileges changed on critical file

New listening port opened

New service activated on payment server

Logging disabled

Medium Priority

New routes added on border router

New local admin user added

Remove The Bad Apples From The Barrel

Remove The Suspicious Or Known Malicious Assets From Your Network

- Isolate or remove suspicious systems from your environment
- Retain copies or the original systems for further analysis
- If you must keep a compromised system running, implement controls to prevent it from infecting other systems
- Determine infection vector and cause using available data

Redeploy Trustworthy Systems

Replace The Bad Systems With Good Ones That Are More Secure

- Recreate systems from trusted sources
- Harden systems to prevent re-infection or repeat compromises
  - Apply current security patches
  - Leverage external standards and hardening guidance
    - SANS / Top 20 Critical Security Controls, CIS Bencmarks, NIST / DISA guidelines
- Determine whether any of your hardening changes should propagate to other systems in the environment
- Remember: Safeguard your automation!

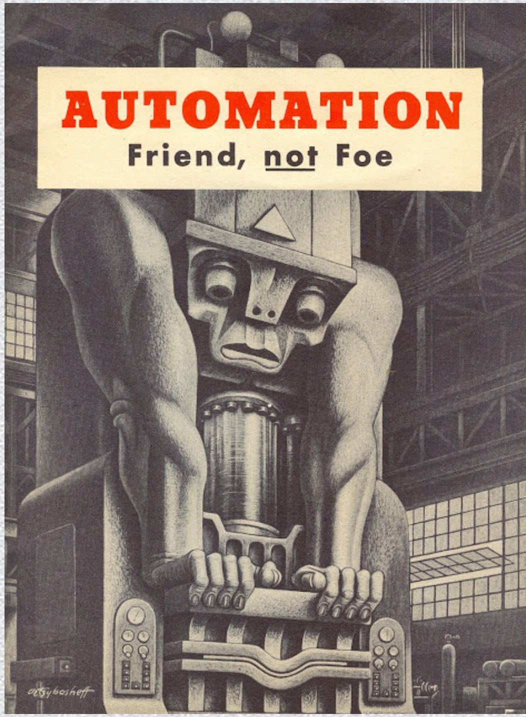
Lessons Learned from the Target Breach

- Importance of Baselines
  - Knowing what “normal” looks like
  - Rapid identification of outliers
- Understanding indirect relationships
  - 3rd-party risk and 3rd-party practices
- Trust but verify
  - Incident response processes
  - Deployment processes
  - Systems
- Communication challenges

Going Forward: Continuously Monitor For Outliers

Continuously Detect Variance And Anomalies So You Aren't Blindsided

- As you deploy and repair:
  - Institute a continuous monitoring strategy
  - Anchor to a known, trusted standard
- Gain benefits in security and availability:
  - Detect variance early
  - Isolate and mitigate incidents before loss occurs
  - Understand patterns to better detect anomalies
  - Shorten time to detection
  - Diagnose efficiently & effectively



Communication Tips

Visibility and consistency builds credibility

Internally…

- Keep business management apprised of your progress
  - Designate a crisis bridge and schedule
- Set milestones and targets based on agreed priorities
- Meet or exceed your targets
- Communicate in language they understand
- Side note: Your communication channels may be compromised – take precautions!

Communication Tips

Visibility and consistency builds credibility

Externally…

- Work with your Legal and PR teams
  - Get external help if you feel you need it
- Inform (and involve) key customers and stakeholders early
- Keep up the cadence of communications
- Create a communication and response plan **before you need one**

Communication Tips

Visibility and consistency builds credibility

Socially

- Decide who your spokesperson(s) will be and maintain consistency
- Explicitly decide / evolve key messages as you get new information
  - Be consistent but avoid speculation, as it will get you into trouble
  - Sharing lessons learned can be a good thing, sharing specific details may not be
- Align your approach so it is consistent with your “brand” and corporate values

A Systematic Approach: Restoring Trust After A Breach

A More Detailed View

- Stabilize the patient
- Know what you have and prioritize by risk and value
- Harvest system state information from your production systems
- Compare what you have to what you deployed
- Remove suspect systems from the environment and return to a trustworthy state
- Continuously monitor and validate to prevent re-compromise
- Communicate in a way that builds trust and confidence

Don’t Be Afraid To Ask For Help

- Be Prepared!
  - Have the “risk conversation” before you’re in an incident
  - AUTOMATION and STANDARDIZATION are your friends
  - Paper exercise a Breach beforehand– involve the organization
- Keep in touch
  - @thatdwayne on Twitter
  - State of Security blog: www.tripwire.com/blog
- Questions?
  - www.tripwire.com
  - highperformer@tripwire.com

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Restoring Trust After A Data Breach

SESSION ID: CDS-W08

Dwayne Melançon, CISA

Chief Technology Officer
Tripwire, Inc.
@ThatDwayne

#RSAC