The Network Effect….

Flipping the Red / Blue Relationship on it's Head

Mike Murray

Sr. Manager

Incident Response Consulting

01 OCT 2019

ISSA Pittsburgh Chapter Meeting

Michael Murray

Senior Manager, Incident Response Consulting

Secureworks' Security and Risk Consulting Incident Response (SRC-IR) Team

About

- Over 15 years of experience in cyber security.
- Focused on delivering proactive incident response services that prepare our clients to act when an incident strikes by ensuring that they have defined, implemented, and exercised the necessary plans and processes, and by augmenting client incident management capabilities during an incident response event.
- Previously Technical Manager for the CSIRT Operations Team at the CERT Coordination Center, Carnegie Mellon University.
- Provided on-site support to U.S. national-level cyber centers to include US-CERT, the Department of Defense Cyber Crime Center (DC3), and Joint Task Force Global Network Operations (JTF-GNO).

Previous Focus Areas

- Public / Private sector information sharing
- International cooperation, National-level CSIRT capability development
- Analysis infrastructure development and deployment
- Operational process and tooling improvements

Passion for Security

- Coordinated collaboration amongst global network of CSIRTs with National Responsibility
- Served on the Forum of Incident Response and Security Teams (FIRST) Board of Directors
- North America FIRST membership committee representative
- Has played a number of roles, starting as junior analyst triaging tickets and answering the CERT/CC hotline
- "Team sport" focus – community, collaboration, information sharing

Agenda

- The Traditional Red “vs.” Blue
- The Network Effect
- Examples
  - Red supporting Blue in Emergency IR
  - Improving Efficacy of Exercises
- Questions

Traditional Red vs. Blue

Red “tests” Blue in the interest of improving Blue…

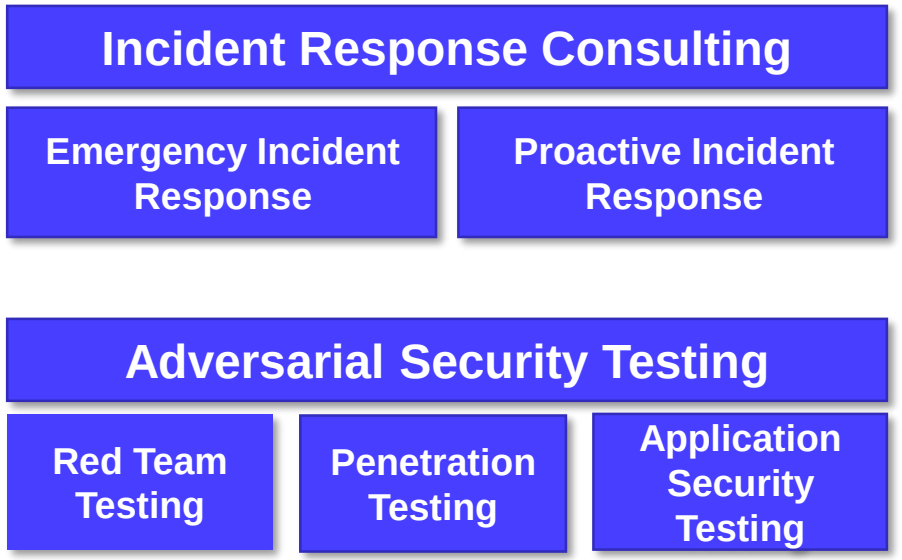
A red team is an ***independent group*** that challenges an organization to improve its effectiveness by ***assuming an adversarial role or point of view***. It is particularly effective in organizations with ***strong cultures and fixed ways of approaching problems***.

https://en.wikipedia.org/wiki/Red_team

This is a key component but has become the focus of the Red / Blue relationship in many cases.

How can we exploit the shared **capability** and **subject matter expertise** to benefit both teams and collectively raise the bar?

Exercise and **assist** instead of **evaluate**.



The Network Effect

Same team, same mission – opposite sides of the line of scrimmage

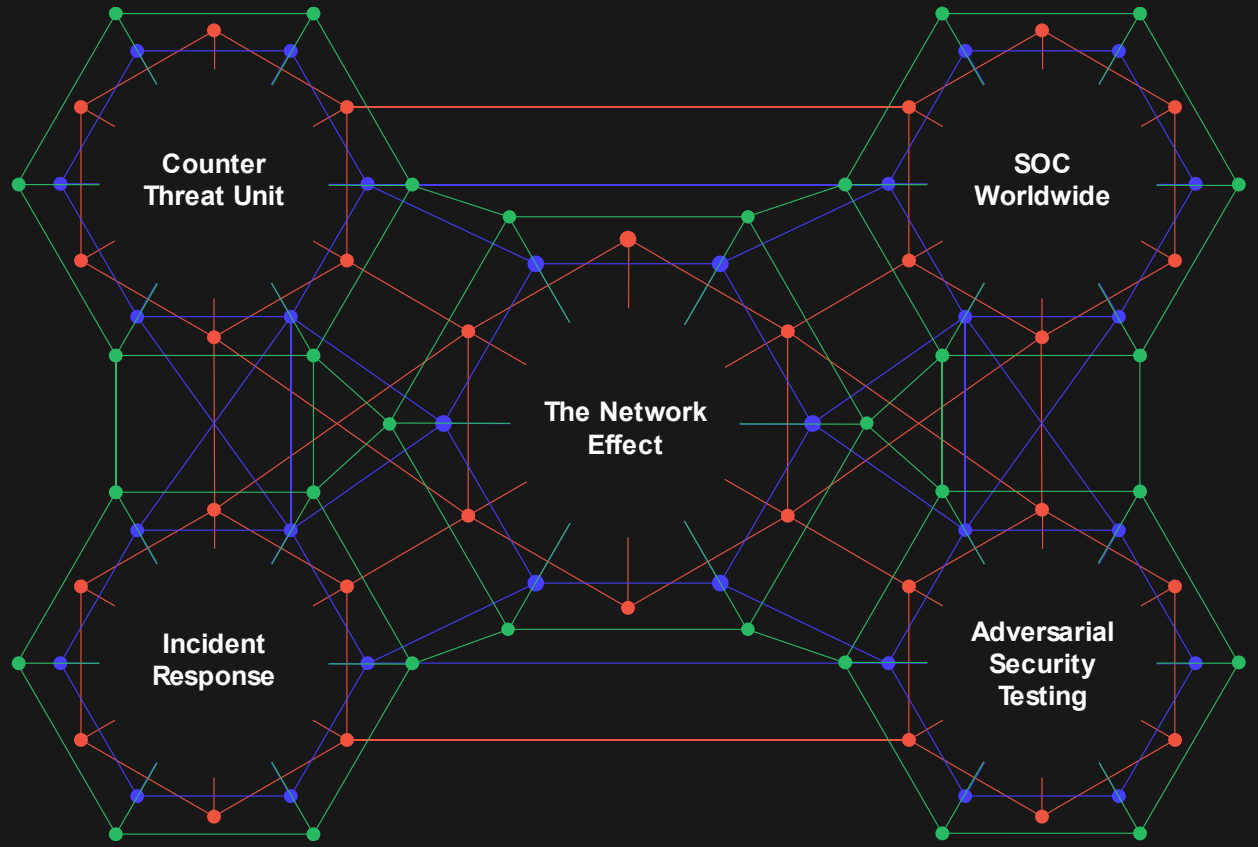
Timely attack surface reduction and control validation during Emergency IR & remediation efforts

Live testing to understand potential root cause of an incident when evidence is unavailable

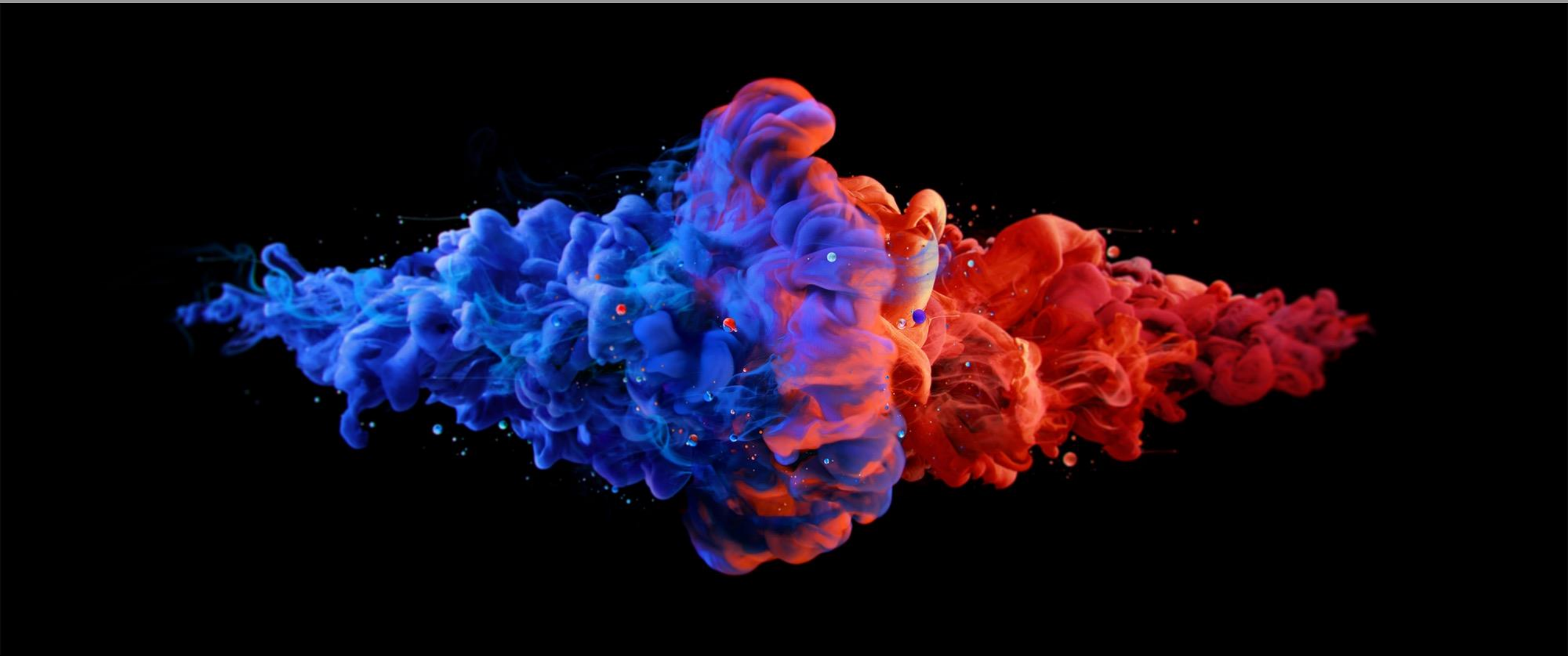
Blue team insights can focus and prioritize Red team efforts for improved ROI, potential to address multiple requirements in one engagement

Greater visibility and insights during functional training exercises – real time collaboration and cross training

Enables both teams to work in their environment – leveraging the tools, processes, and capabilities that they will have access to during an actual incident



Red supporting Blue in Emergency IR



Ransomware – The Good and The Bad

The New York Times

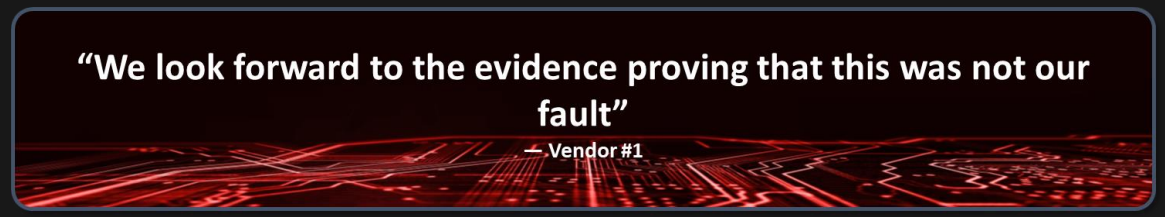
Threat researchers at Dell SecureWorks, the Atlanta-based security firm helping the city respond to the ransomware attack, identified the assailants as the SamSam hacking crew, one of the more prevalent and meticulous of the dozens of active ransomware attack groups. The SamSam group is known for choosing targets that are the most likely to accede to its high ransom demands — typically the Bitcoin equivalent of about $50,000 — and for finding and locking up the victims' most valuable data.

eCommerce Application Compromise

Vendors Gone Wild

Scenario: Client is dealing with un-cooperative vendors, and needs to restore operations ASAP

- Each vendor aggressively out to prove it wasn't their fault
- Wild conclusions about the cause, and nasty accusations over the phone
- What does the available evidence tell us?



Evidence of SQL injection attempts against admin accounts, with the intent of bypassing authentication

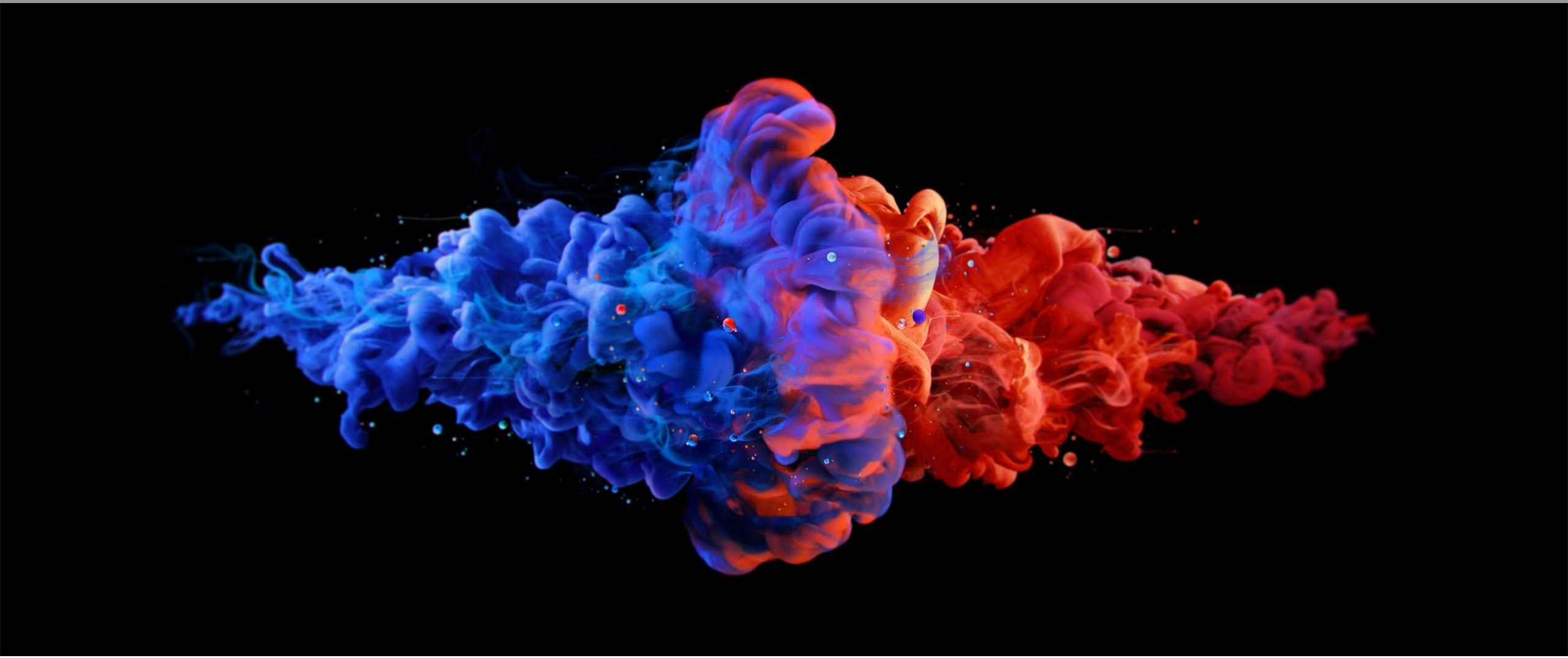
- Vendor #1 declares this is proof of how the attack began
- All previous logins to admin accounts were from the US, with one exception

Logs shows NONE were successful

Eventually granted testing permission & with some poking identified SQL injection against an unauthenticated parameter

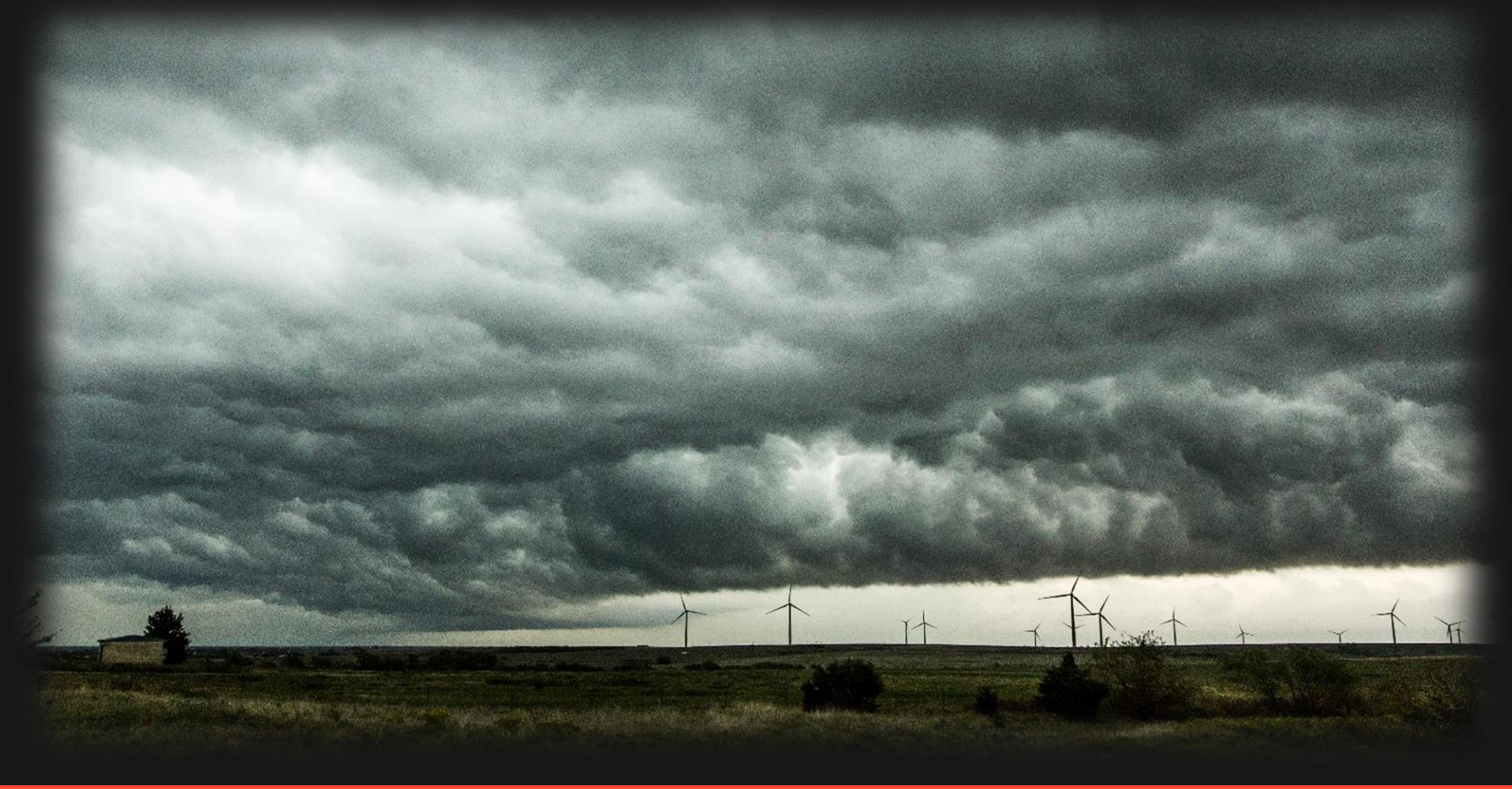
- Blind, so a LOT of requests
- They show the retrieval of admin hashes
- Shortly after, our compromised account was logged into from Sweden
- This was an account managed by vendor #1 that had been dormant for almost 2 years

Improving Efficacy of Exercises



Preparing for a Storm

Leverage the forecast to focus your defenses



Point-in-time Functional Exercising

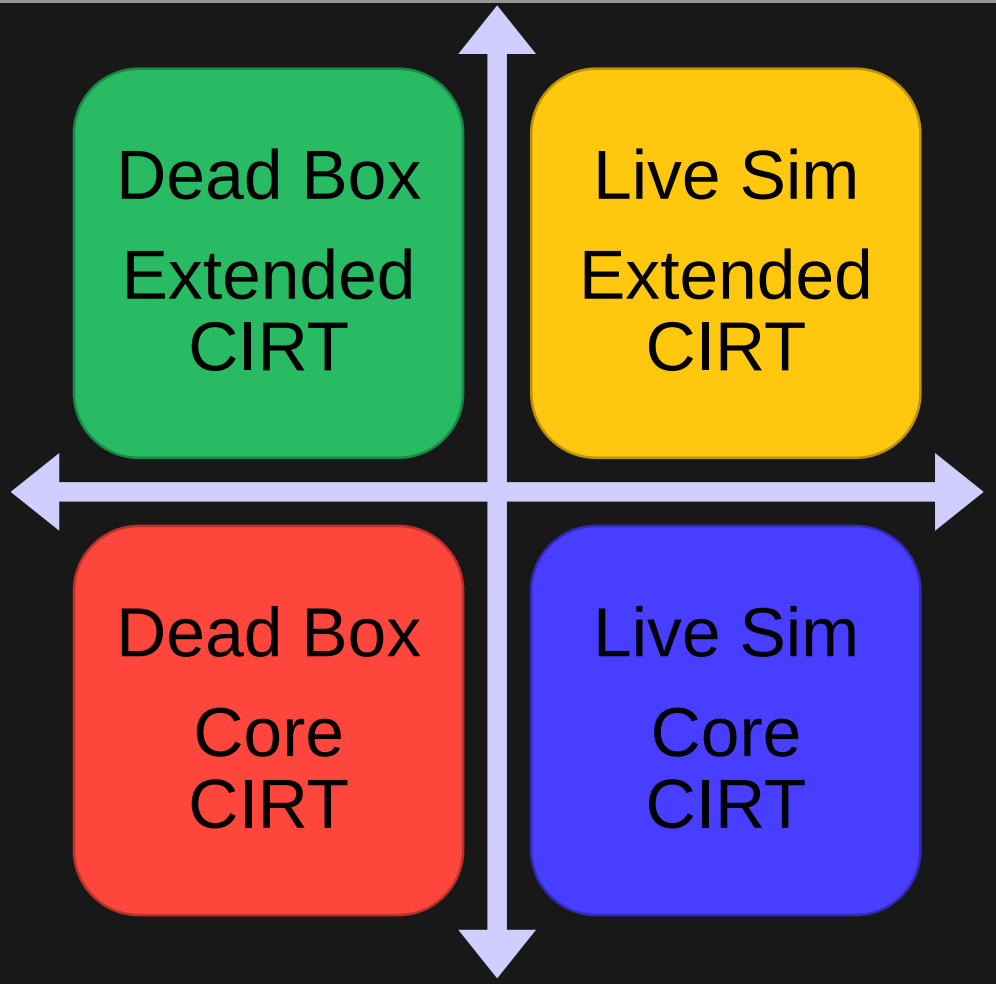
Beyond the tabletop…

IR Functional Exercises allow personnel to validate their technical readiness by performing their actual hands-on duties in a simulated manner.

- **Live Simulation** – Adaptive to the client environment, and all tools available.
- **Dead Box** – Prebuilt scenario, limited tools available

- **Core CIRT** – Technical level participants
- **Executive level CIRT** – Both Technical and Enterprise level participants (full spectrum)

These tend to have multi-day duration and are expensive from a resource consumption perspective.



CADET

Security Beyond Audit

> "That's what games are, in the end. Teachers. Fun is just another word for learning."
> — Raph Koster, Theory of Fun for Game Design

Red Team

- **Evaluates** people and processes
- Point-in-time scope
- Score determined by number of objectives Red Team completes
- Tests generally occur once or twice per year
- Reports are large (150+ pages)
- Reports focus on narrative and techniques
- Client involvement is low to moderate
- Adversary capabilities are regulated by scope and time

CADET

- **Exercises** people and processes
- Continuous scope
- Score determined by defensive detection and response times
- Scenarios executed weekly, bi-weekly, or monthly
- Reports are small (~15 pages)
- Reports focus on events and indicators
- Client involvement is moderate to high
- Adversary capabilities are regulated by scope and scenario

In Summary

Foster and exploit the broader capability of your teams

Build relationships across the aisle. Strive for Red / Blue relationship to be collaborative, not [always] adversarial.

Leverage Red to validate Blue activities and identify additional gaps during active IR activities.

Enable cross-pollination of subject matter expertise and shared domain mentoring opportunities.

Thank You!

Read the Report

Incident Response Insights Report 2019

Secureworks' Risks, Remedies, and Best Practices for Defending Against Cyber Threats

Read the Blog

Can Your Vendor Provide Support During a Cybersecurity Incident?

Learn what actions can best help prepare for an incident involving external vendors

Read the White Paper

Planning an Effective Incident Response Tabletop Exercise

Learn how to make the most of your investment in tabletops and common pitfalls to avoid

Listen to the Webcast

Improving Incident Response Outcomes

How to defend faster and reduce risk more effectively in the face of a cyberattack

Listen to the Webcast

Proactive Incident Management
An Eyes-Wide-Open Approach to Cyber Security - best steps to mitigate risk before a breach occurs

Read the White Paper

9 Key Questions to Ask an Incident Response Provider

Assess a provider's IR capabilities and know if they're a good fit for your security program

Learn More

Emergency Incident Response
Proactive Incident Response
Incident Management Retainer