



# Attack Demo

August 16, 2018



## EXPERTISE

**100+**  
EXPERT ADVISORS  
& CONSULTANTS

 **50+**  
FORENSICS & SECURITY  
CERTIFICATIONS

**LARGEST FCPA**  
INVESTIGATION IN  
HISTORY

**10 RELATIVITY**  
**MASTERS**  
MORE THAN ANY  
OTHER COMPANY

**50+**  
SECOND  
REQUESTS  
COMPLETED

## SCALE

**60+**  
OFFICES, DATA CENTERS & REVIEW  
FACILITIES IN **11 COUNTRIES**

  
**2,500**  
EMPLOYEES WORLDWIDE

  
**2,300+**  
SEATS OF  
REVIEWER CAPACITY

 **100K+**  
SUCCESSFUL CLIENT  
MATTERS & COUNTING

 **1B+**  
PAGES REVIEWED  
IN LAST 2 YEARS

## TECHNOLOGY

### CERTIFICATIONS:

- SOC 2 TYPE 1
- SOC 2 TYPE 2
- SOC 3
- ISO 27001



FROM THE  
NATIONAL LAW  
JOURNAL

  
**30+**  
PETABYTES  
UNDER  
MANAGEMENT

 **14+**  
DATA CENTERS  
AROUND THE WORLD

**RISKCOVERY**  
 **sightline**  
by Consilio

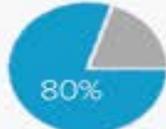
## CUSTOMER FOCUS

 95% **95** OF THE  
AMLAW 100 AS CLIENTS

 **#1**  
NPS SCORE  
IN INDUSTRY



COUNTRY MATTER  
EXPERIENCE

 80% **16** OF TOP 20  
TOP FINANCIAL SERVICES  
FIRMS

**7,000+**  
MATTERS CURRENTLY HOSTED

## Information Security Offerings

- IT systems audit services (CSC Top 20, ISO 27001 aligned)
- Vulnerability assessments
- Penetration testing (internal/external/wireless/web)
- Data incident investigation & response
- Indicators of compromise scan

## Other Offerings

- Data destruction/de-identification
- eDiscovery
- Secure hosting and review

## **BROCK BELL, GCFA, GNFA, DFCA, GCIH, CCPA, ACE, Security + INFORMATION SECURITY RESPONDER**

Brock Bell currently serves as an information security responder for Advanced Discovery/Consilio. Brock has worked in the private sector with Fortune 100 corporations, AM Law 100 firms, political campaigns, and government agencies to provide analysis for matters of intellectual property theft, corporate espionage, and incident response. Brock has experience collecting data from and performing in-depth analysis of many operating systems and infrastructure platforms. Prior to working for Advanced Discovery (formerly Altep), Brock served as a security analyst for a national trucking, shipping, and warehousing logistics company. In 2014, Brock helped create the Digital Forensics Certified Associate (DFCA) certification as part of the Digital Forensics Certification Board (DFCB). Brock currently sits on the Digital Forensics Certification Board as co-chair of marketing and communications.

## **ANDREA DOMINGUEZ, GNFA, GCIA, GCIH, GSEC, SSCP, CAPM INFORMATION SECURITY ENGINEER**

Andrea Dominguez currently serves as an information security engineer for Advanced Discovery/Consilio. Andrea has extensive Security Operations Center (SOC) experience in the financial industry. Her experience includes incident response, network forensics, security operations, phishing campaign investigation, threat intelligence, network and endpoint monitoring, and phishing tests, among others. Prior to working for Advanced Discovery, she worked at a Fortune 100 corporation. Andrea is currently pursuing a master of science degree in information security engineering (MSISE) through the SANS Technology Institute, the graduate school portion of the SANS Institute, which is the most trusted information security training provider in the industry. She holds several GIAC certificates in security topics such as network forensics and intrusion analysis.

# Scenario 1: Introduction

## Phishing and Data Exfiltration

- Reconnaissance
- Phishing email
- Credential harvesting
- Reuse credentials for domain
- Lateral movement
- Unauthorized access to data
- Data exfiltration
- Extortion

# Scenario 1: Demo

## Phishing and Data Exfiltration

Demo

# Scenario 1: Recommendations

- Do NOT reuse passwords
  - Password management programs can help you maintain unique, secure passwords
- Phishing tests and security awareness training
  - Foster a culture of reporting suspicious emails
- Do NOT store sensitive files in terminal services server
- Technical protections:
  - Web proxy/filter
  - Email filter settings
- Multi-factor authentication
- Logging/Sysmon
- Endpoint protection (HIDS/HIPS)

# Scenario 2: Introduction

## Remote Access and Ransomware

- Publicly available RDP
- Brute force weak admin credentials
- Access terminal server through stolen credentials
- Lateral movement
- Install ransomware
  - Extract ransom for decrypting data

## Scenario 2: Demo

### Remote Access and Ransomware

Demo

# Scenario 2: Recommendations

## Remote Access and Ransomware

- Enable Network Level Authentication (NLA)
- Do NOT have external-facing RDP services available
- Back up your data
  - Have a plan for how to restore – test frequently
- Network IDS/IPS
- Credential management
  - Enforce secure (complex) passwords
  - Non-default administrator usernames
- Multi-factor authentication
- Network segregation/VLAN

Thank you



Any questions?

