

The FireEye logo is positioned in the top left corner, enclosed within a thin white circular border. The background of the slide features abstract geometric shapes in shades of red, black, and white, creating a modern, tech-oriented aesthetic.

FireEye®

Hunting & Intel

How to Get Amazing Results from
Existing People & Technology

Steven Booth

CSO, FireEye

February 26, 2019

Ground Rules



CAPABILITIES

not products or features



REALITY

All situations are real, from real customers



INTEL & HUNTING

are bastardized terms

Process – Intelligence Consumption:

 **INTEL
REQUIREMENTS/
TRIGGER**

 **INTELLIGENCE
GATHERING**

 **DECISION**

 **OPERATIONALIZE**

**APT29 Doing Evil
Delegations in O365**

**How Much Do
We Care?**

- Analyze Delegations

What Do We Do?

- Build Hunt

**How Do I Make
This Easier?**

- Automation

Phishing Campaigns to Predictive Security

 **INTEL
REQUIREMENTS/
TRIGGER**

 **INTELLIGENCE
GATHERING**

 **DECISION**

 **OPERATIONALIZE**

Phishing campaign linked to APT34

- Spear Phishing Campaigns → attribution

- Office 365 / Okta Lock Out

How Much Do We Care?

- APT 34

- Hardcore IR

What Do We Do?

- Pivot on TTPs (Cred Harvesting)

- Hardcore Remediation

How Do I Make This Easier?

- Repeat

- Beer

APT28 Lateral Movement

INTEL REQUIREMENTS/TRIGGER

INTELLIGENCE GATHERING

DECISION

OPERATIONALIZE

APT 28 Lateral Movement

How Much Do We Care?

What Do We Do?

How Do I Make This Easier?

- Attack Lifecycle

- Hunt for psexec or cryptomining

- Convert to SIEM Analytic

- Hardcore IR

- HX & Smart Vision

- Convert to SIEM Analytic

MAINTAIN PRESENCE

- CHOPSTICK
- DARKMIRROR
- NIGHTCALL



MOVE LATERALLY

- PSEXEC
- ETHERALBLUE
- XTUNNEL



- Phishing
- Credential Theft
- WiFi Sniffing
- GAMEFISH
- BOSSNAIL
- SOURFACE
- OLDBAIT
- Mimikatz
- Secretsdump.py
- Responder
- Port Scanning
- Compress & Exfiltrate data
- Delete log files

I'm a Customer Who Uses AWS — How Can FireEye Help Me?

MANDIANT

INCIDENT RESPONSE



COMPROMISE ASSESSMENT



SECURITY PROGRAM ASSESSMENTS



NETWORK



FIREEYE NETWORK SECURITY



Testing & Visibility



Network & Security Convergence

AWS CONSOLES



CORPORATE NETWORK

ENDPOINT



VM Linux



VM Windows



VM Mac

HELIX



CLOUDTRAIL



S3



ELB



