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

How Much Do We Care?

- APT 34

What Do We Do?

- Pivot on TTPs (Cred Harvesting)

How Do I Make This Easier?

- Repeat

- Spear Phishing Campaigns → attribution

- Office 365 / Okta Lock Out

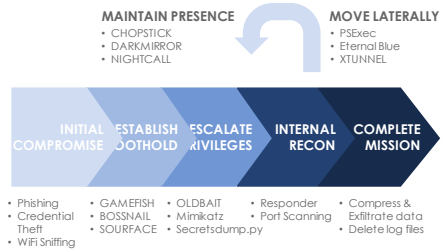
- Hardcore IR

- Hardcore Remediation

- Beer

APT28 Lateral Movement

APT 28 Lateral Movement



INTEL REQUIREMENTS/ TRIGGER

INTELLIGENCE GATHERING

DECISION

OPERATIONALIZE

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

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

MANDIANT

INCIDENT RESPONSE

COMPROMISE ASSESSMENT

SECURITY PROGRAM ASSESSMENTS

NETWORK

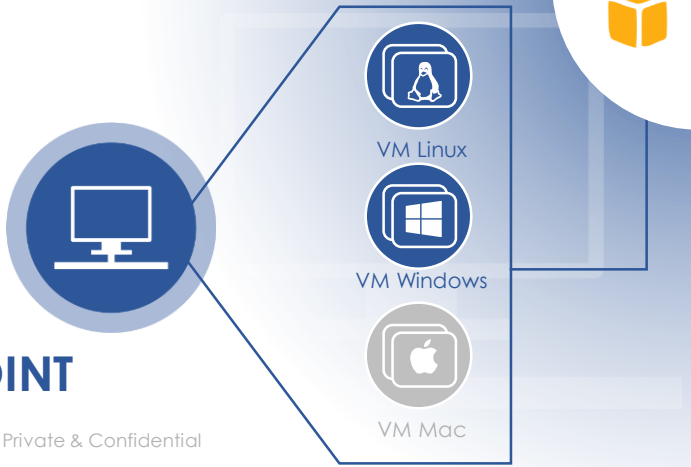
FIREEYE NETWORK SECURITY

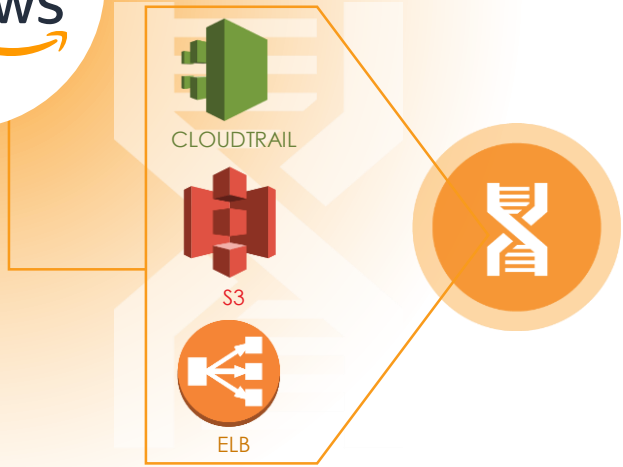
ixia Testing & Visibility

Gigamon Network & Security Convergence

AWS CONSOLES

CORPORATE NETWORK





ENDPOINT

HELIX