



# DEFENDING ACTIVE DIRECTORY WITH WIRE DATA

---

Leverage shared data and  
tools to optimize budgets and  
improve end-user experience

Vince Stross  
Principal Security Engineer  
ExtraHop

# DEFENDING ACTIVE DIRECTORY WITH WIRE DATA



## Active Directory activity you can see on the wire:

- Invalid Passwords
- User Lockouts
- Disabled Accounts
- Time Skew Errors
- Policy Rejected
- Unknown SPNs
- New Privileged Access
- Privileged Access Errors
- DNS Service Records
- Global Catalog Records
- LDAP Plain Text Binds
- Group Policy
- DNS Service Lookup Processing Time
- High Global Catalog Processing Time
- High Kerberos Processing Time

# DEFENDING ACTIVE DIRECTORY WITH WIRE DATA

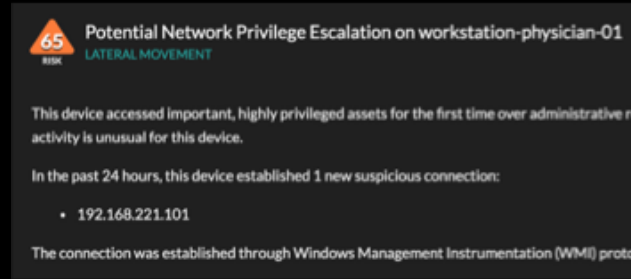
## Attack Detection

Behavioral analysis to detect attacks at various stages



## Privilege Escalation

Machine learning to understand privilege and detect escalation



## Account Monitoring

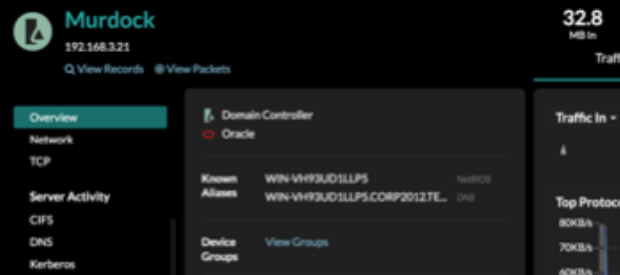
Continuous passive observation of user and account activity

User Name: admin | 4 active users

Name	Devices
admin	AccountingLaptop
administration	AccountingLaptop
administrator	Barnysdale, WINDOWS-8-1, WINDOW-XP-1, WINDOWS-10-
adminsqli	AccountingLaptop

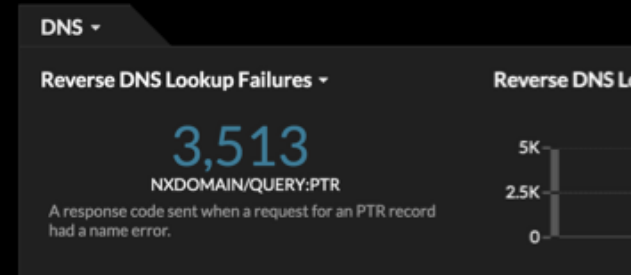
## Identification of Rogue Devices

Passive device auto-discovery and classification



## Policy Compliance Monitoring

Customizable alerts and dashboards to monitor policy compliance



## Network Forensics

Drill down to transaction records and the constituent packets

Packet Query

From Apr 7, 11:00:00 pm

BPF = ((host 192.168.221.102 and port 57611) and (host 192.168.221.21 and port 445)) or (host 192.168.221.102 and po

BPF: Add Filter | 269,988 packets

Previewing 20 packets around Apr 8, 4:22:46.287 am

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags
2019-04-08 04:21:01.036	192.168.221.102	192.168.221.21	TCP	57611	445	ACK
2019-04-08 04:21:01.036	192.168.221.21	192.168.221.102	TCP	445	57611	ACK
2019-04-08 04:21:31.116	192.168.221.102	192.168.221.21	TCP	57611	445	ACK

**DEMO**



Rise Above the Noise.

Online demo available at [www.extrahop.com/demo](http://www.extrahop.com/demo)