ExtraHop

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

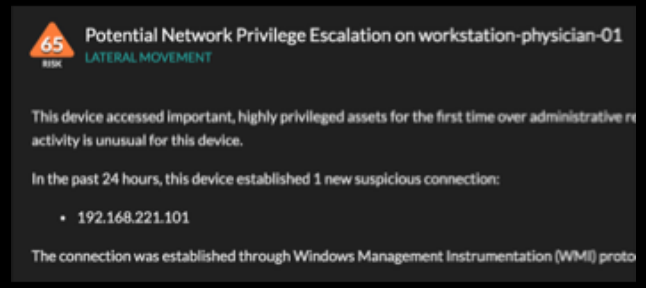
DEFENDING ACTIVE DIRECTORY WITH WIRE DATA

Attack Detection

Behavioral analysis to detect attacks at various stages

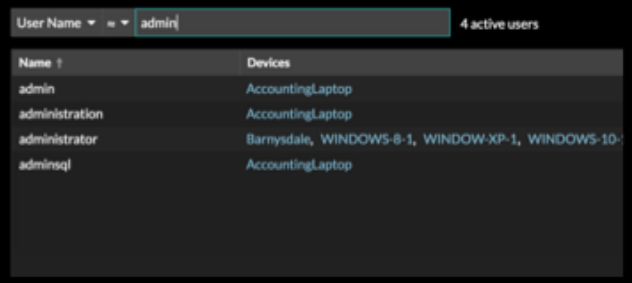
Privilege Escalation

Machine learning to understand privilege and detect escalation



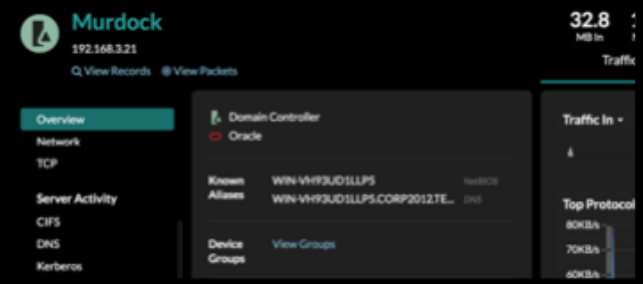
Account Monitoring

Continuous passive observation of user and account activity



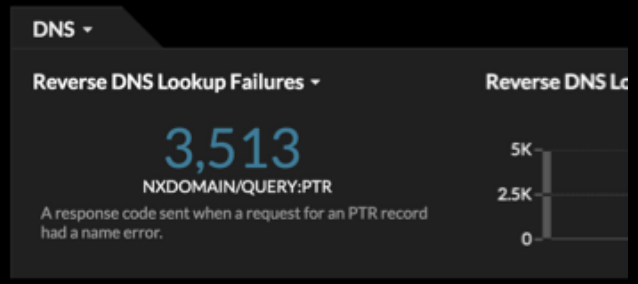
Identification of Rogue Devices

Passive device auto-discovery and classification



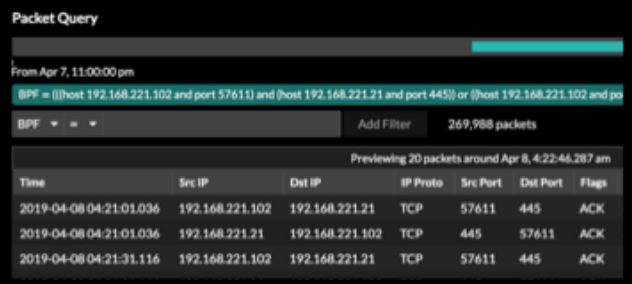
Policy Compliance Monitoring

Customizable alerts and dashboards to monitor policy compliance



Network Forensics

Drill down to transaction records and the constituent packets



DEMO

Rise Above the Noise.

Online demo available at www.extrahop.com/demo