How to Achieve a 5 Minute MTTD by Detecting at the Source

Sean Scott– Manager of GreyMatter Operations

RELIAQUEST

EXPONENT

Challenges with SIEM-Centric Detection

Slow and Manual Updates:

- Requires data to be parsed, indexed, and stored before you can run detection queries

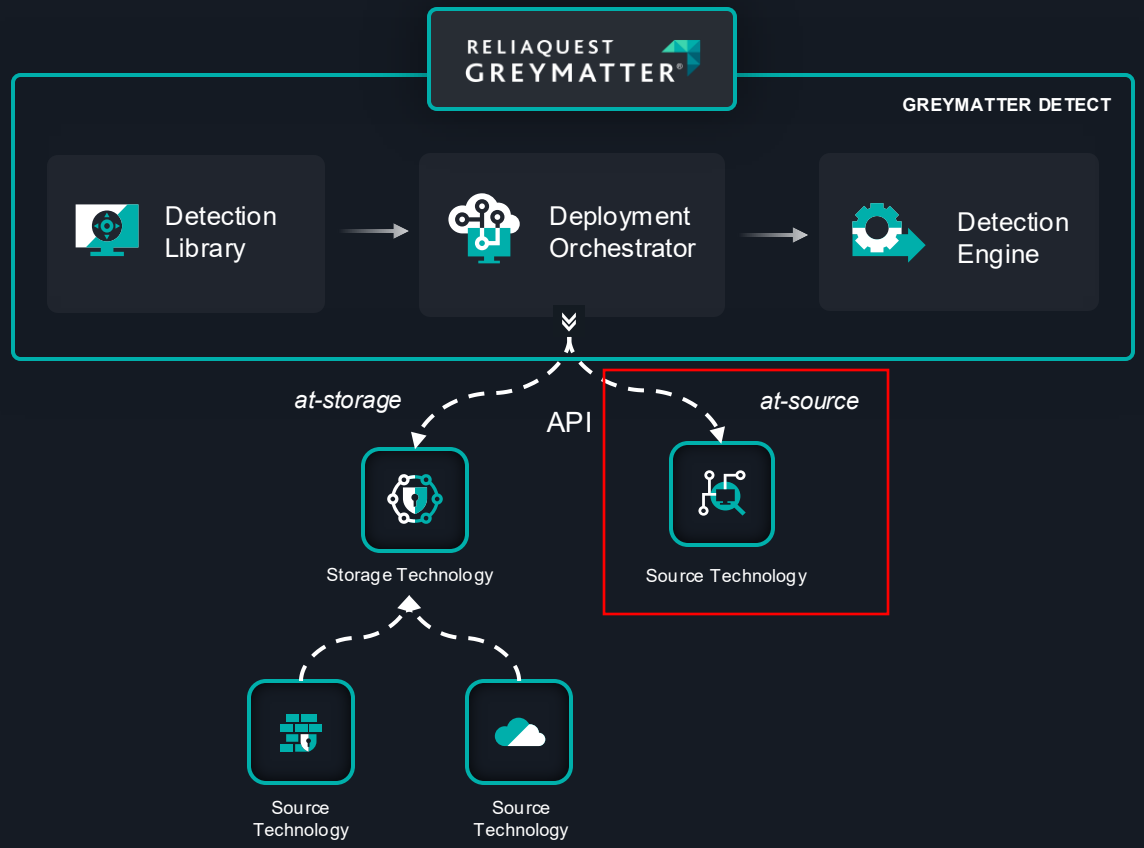
Flexibility Limitations:

- Difficulty retaining detection coverage while swapping out technologies or migrating SIEMs

Resource Constraints:

- Different technology languages and capabilities require specialized expertise.

Detect in Minutes Across SEIM, Cloud, Endpoint, Network, and Email Without Storing Data.



- GreyMatter connects to technologies via API to remotely execute the detection logic from the Detection Library and generate an alert.
- GreyMatter can detect directly at the source technology or through a storage technology, or a combination of both.

Detect at-source

Swap Techs, Same Coverage

Reduce Ingest Costs and Accelerate Detection

Real-World Examples & Use Cases

Mergers and Acquisitions:

- GreyMatter can quickly integrate and coordinate threat detection across various vendor tools from both entities, providing rapid coverage with unified visibility and control.

Hybrid Environments:

- GreyMatter can bridge the gap by connecting to both cloud and on-premises and deploying detection across the environment for unified visibility and scale.

Emerging Threats:

- GreyMatter immediately deploys updates of detection logic based on new threats across all your technologies. Additionally, GreyMatter leverages threat intelligence feeds for real-time detection updates to stay ahead of adversaries.

RELIAQUEST

EXPONENT

Thank you

www.reliaquest.com

800.925.2159

info@reliaquest.com