



# KEY USE CASES

## SIEM Alternative

Move past costly solutions and avoid data lock. Make the most out of your existing tools without rule-writing with Hunters' automatic investigations that reduce detection analysis and triage time to seconds instead of minutes or hours.

## IR and Threat Hunting

Uncover root cause analysis and gain unprecedented situational awareness through cross-surface correlation, or implement your own hunting theses using Hunters' graph to query your environment for malicious activities.

## Security Data Lake

Scale with your business needs with unlimited storage at a fraction of the cost. Leverage Hunters XDR to lift and shift all your security data and use out-of-the-box analytics to make sense of your telemetry.

# HOW IT WORKS

**Seamless, Flexible Ingestion:** +C973?E43?>>53D7ECD?@Q59D75H0D97C53EBD D?C?B4Q53D:3?>>53D97D)I#`·  
f E>D5EC./ (3?<53C?7C5F5>D1>4D5=5D6? =4?J5>C?641D1C?EB35C?>@B=Q5C1>49D853?E493E497fV(C`  
\$/ (C i ?E4C5F985@B?F945BC Q25G1<C Z45>D9D 1>4, 335CC= 1>175= 5>DD?C 1>4= ?B5

**Detection Engine:** f E>D5EC./ (5H0B130CDB51DC9>1<C1>415B0C? = @5D121D5C?65H0D97C53EBD 41D1EC971D851=  
@B?35CC971>14D2C D538>? ?71 ZD5>12<C>51BB51<D9 5@B?35CC971>43? = @5H1>14D2C \*8B51DC9>1<5H0B13D9>C  
7E945421 f E>D5EC \*\* & 21C541D13 9D5<G 8988C1C? = 1@54?>D 1# Z (fi, \*\* i! D538>9AE5

**Data Representation on a Multi-Dimensional Graph:** \*85D5=5D6?3?<53D54? = F1B7ECZ\*1>4C53EBD D?C?C?  
5653D954 3?>>53D54 D 75D85B?>1@B?@B5D1B ! >?G 5475L B1@8 1CDE3DEB4 B5@B5C>D1D9 >?61<D85CEC@99EC  
2581F9EB1<D855>D99C9 D85>5D6?B 1>4D85B54D9>C89C25D655>D85=

**Automatic Investigation:** Z?B45BD E>45BD1>4G51; D851DC9>1<C1>415B0C f E>D5EC E>C1ED? = 1D99F5091D9>C ZD  
6D85C1<B55F1>D96B= 1D9>1CC?391D54 G Q8B8?C5 93E497 61DEB5C1>45>D99CDB1DG 5B59F?F549 1C@5398  
CEC@99EC13D9D 1>41ED? = 1D81 4 5>B285CD85= G Q8 6B85B3?>D5D

**Scoring and Prioritization:** %>35D85B5?C5>?E783?>D5HD1B?E>4 D851DC9>1<C1>415B0C f E>D5EC./ (5F5B175C# " D`  
C3?B5D85= ? = ` D` 1<G 978B1>51D @B?B991D9>

**Cross-Surface Correlation:** f E>D5ECE5CE>CE@5B?Q54 51B97 D?3?B54D5C9>1<C1>415B0C13B?CC4Q@1B1D51B51C?6  
CEC@99EC13D9D 9 D85L B1@8 57 CE@53D54 @8Q8975= 196 <G 5421 = 1G 1B54?G>?14C?>71D5G11 1>4fV ( `·  
1>4CEB13513D9>125, D13 ) D?B5CG 898893E456<1D13 CE= = 1B 1>4?ED95

**Response and Remediation:** ) D851= 9545D53D9>1>4B0C@?>C521 5C314D97, D13 ) D?B5C9D? )%, ( D?<C1>4?D85B  
5H0D97G?B 6?GC 5>1297B0C@?>C51ED? = 1D9>1>4B54E3971D13 5BC 4G5<D9 5

# KEY INTEGRATIONS

Integrations span across security products, data connectors, and workflows.



See all of Hunters' Integrations and Technology Partners here.