

A person is running on a treadmill in a gym. The camera angle is low, focusing on the person's legs and feet. They are wearing black and red sneakers. In the foreground, a computer keyboard is visible, suggesting a connection between physical activity and technology. The background is slightly blurred, showing a window and gym equipment. The overall lighting is cool and blue-toned.

MAKING YOUR SOC RUN

 **Hunters**



Legacy SOCs are failing

Stuck on the SOC Treadmill

*New Attack
Vectors*

*Data
Explosion*

*Growing
Costs*



MSSP is just a band-aid

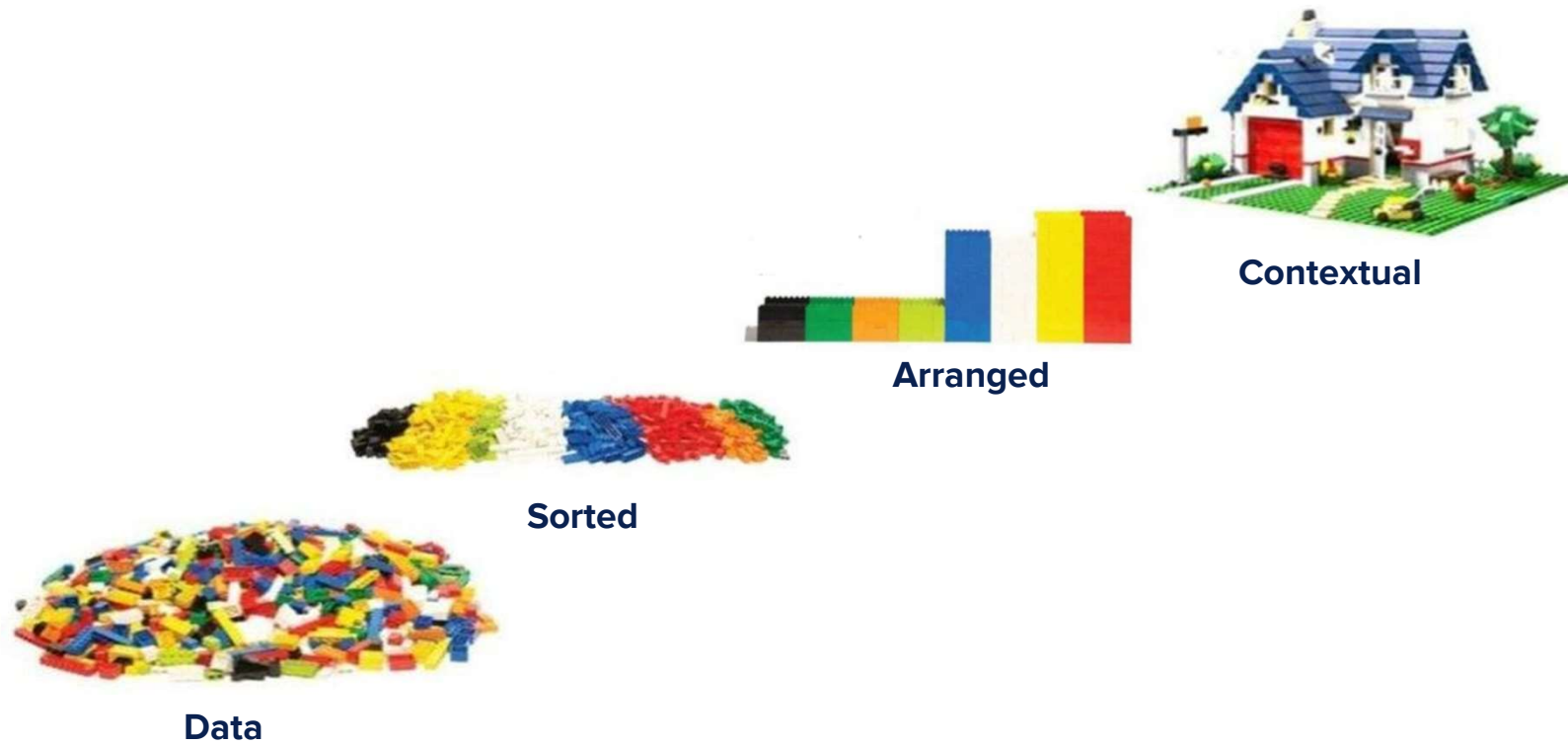
Too noisy on routine, Too silent upon a breach

*Rely on legacy
SIEM*

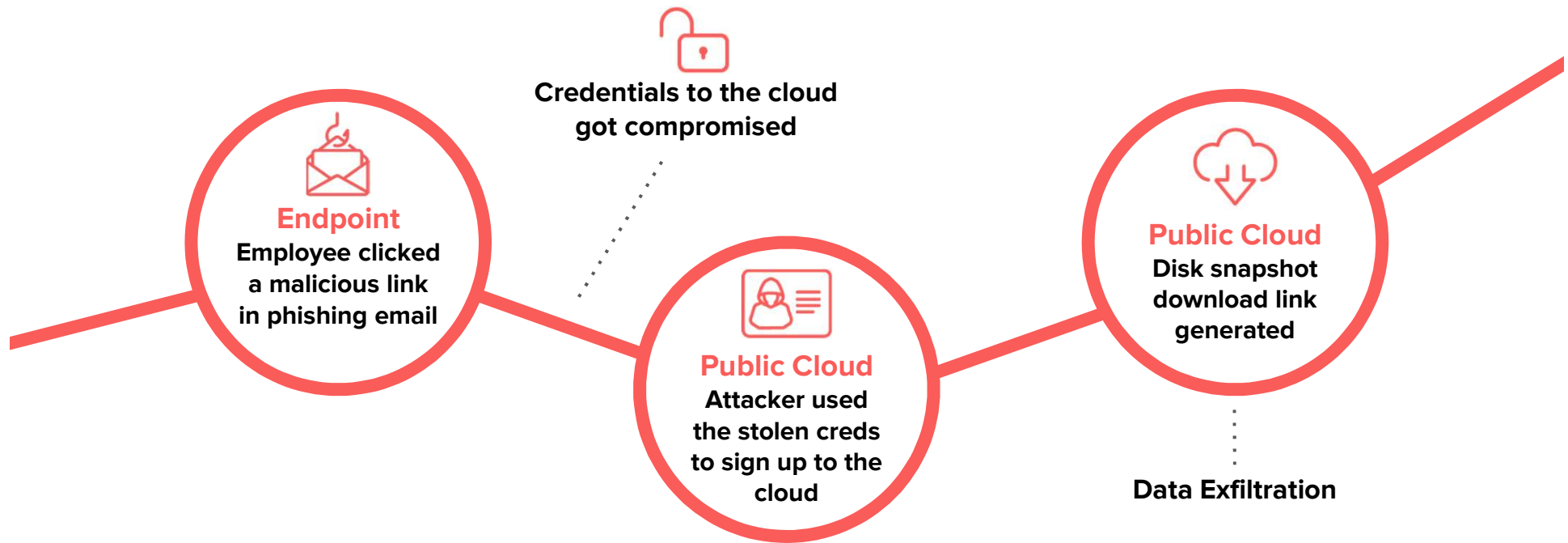
*Rely on
manual work*

*Rely on
your team*

How Does Your SOC Run Today?



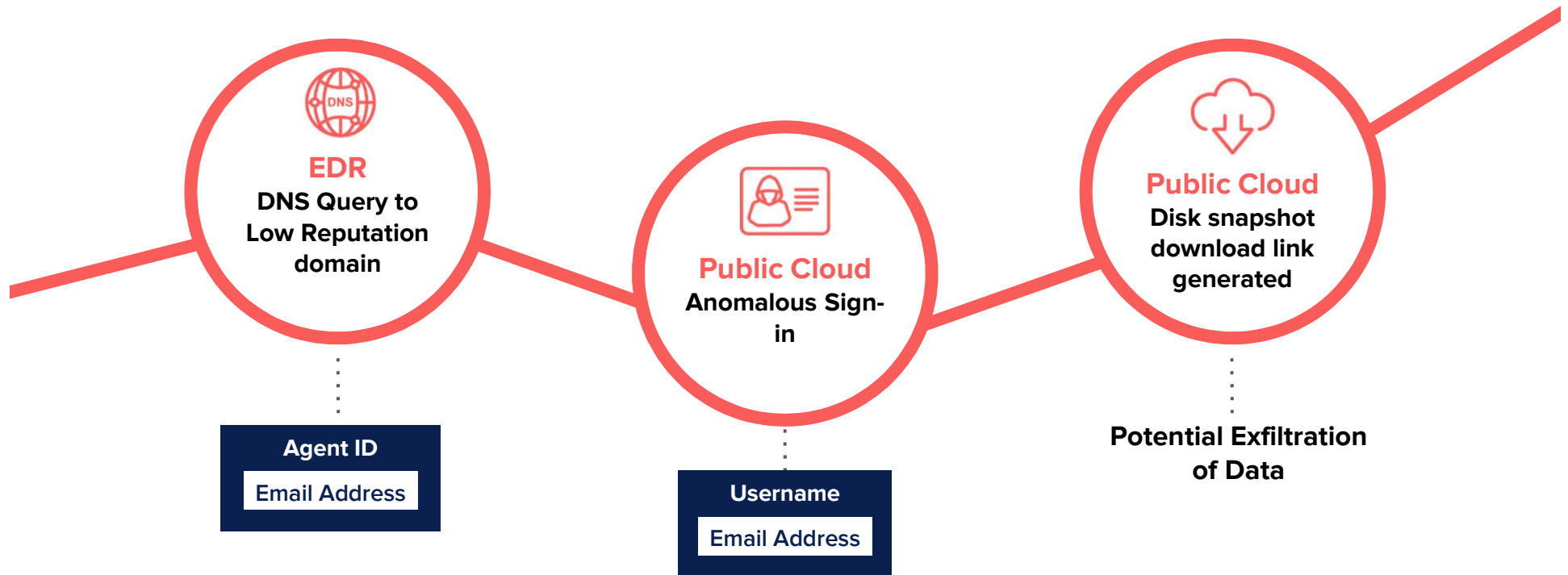
An Attack Story



Disjointed Signals, Likely to be Ignored

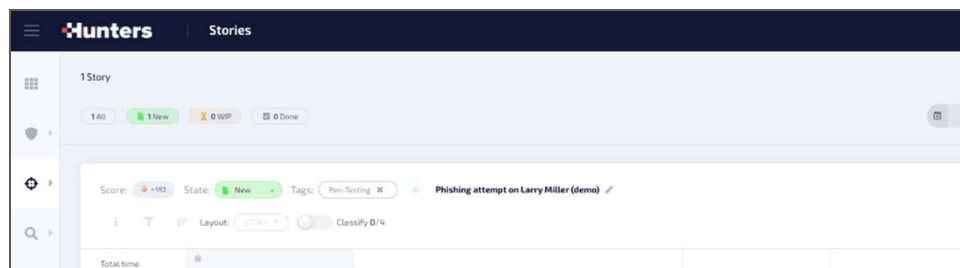


Hunters XDR: Connecting the Dots



Hunters XDR

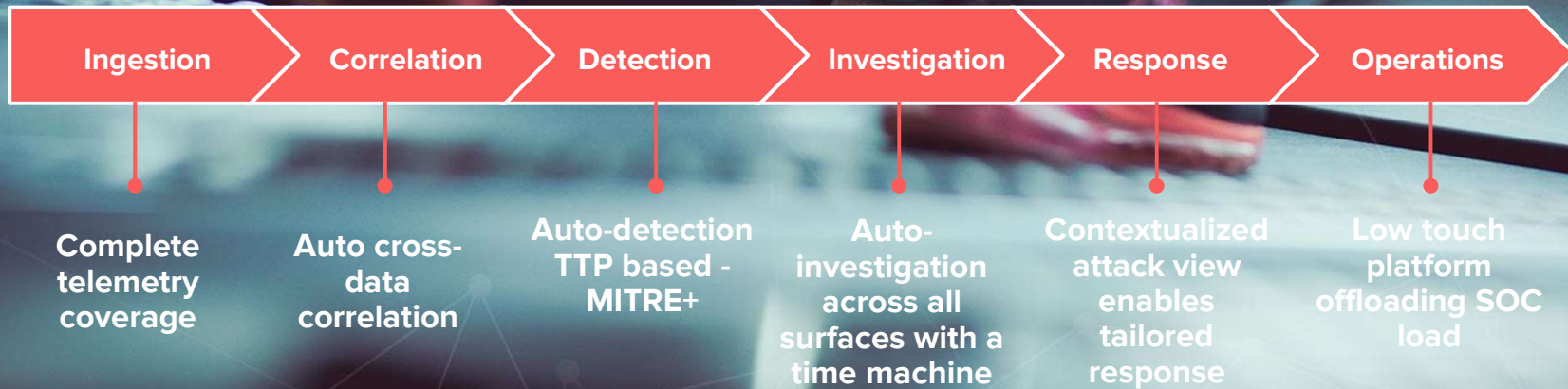
Attack Stories



	WHO	WHAT	WHERE
<p>Total time 28 min, 22 sec a year ago</p> <p>13:31 Apr 3</p> <p>+18 DNS Query to low reputation domain #crowdstrike-raw-events 1 lead</p>	<p>Process ID 385971230036</p>	<p>Requested Domain hunters-ss0.xyz</p>	<p>CS Agent ID 2a92...55e7</p>
<p>+56 Azure AD Sign-in Marked as Risky by Microsoft #azure-signin 1 lead</p>	<p>Properties User Principal Name larrymiller@hunterslab.onmicr</p> <p>Caller IP Address 142.93.65.54</p>	<p>Properties Risk Detail userPassedMFADrivenByRiskBz</p>	<p>Properties App Display Name Azure Portal</p>
<p>+50 Azure Disk Snapshot Download Link Generated #azure-activity 1 lead</p>	<p>Person Name Larry Miller</p> <p>Caller IP Address 142.93.65.54</p>		<p>Azure Appid c44b4083-3bb0-49c1-b476-97</p>

WHAT	WHERE
Requested Domain hunters-ss0.xyz	CS Agent ID 2a92...55e7
Properties Risk Detail userPassedMFADrivenByRiskBz	Properties App Display Name Azure Portal
	Azure Appid c44b4083-3bb0-49c1-b476-97
	Azure Appid c44b4083-3bb0-49c1-b476-97

Run SOC, Run...



Hunters

How Does Hunters Transform the SOC?



Extend Data Usability



Gain Incident Clarity



Elevate Business Impact

Key Outcomes

1

Cut through the noise

with rich endpoint telemetry extended into new attack surfaces

2

Reduce detection and triage time

with Hunters' enrichments, scoring and prioritization

3

Investigate faster

with correlated endpoint telemetry from CrowdStrike

4

Expedite incident response

with root-cause analysis, and gain additional risk awareness and insights into multi-surface incidents

5

Empower sophisticated threat hunting

leveraging detections of weak threat signals that bypass siloed organizational defenses

Hunters FREE Cyber Expert Consultation

Get insights on how to improve your ingest-detect-respond workflow

Visit Booth 7-110b in Hall 7