### **Sentinel**One<sup>®</sup>

### Human Machine Teaming: Why the human element will always be indispensable in Cybersecurity.

Martin Knopf Senior Systems Engineer, SentinelOne

### Will robots take your job? Humans ignore the coming AI revolution at their peril.

### **STEPHEN HAWKING WARNS ARTIFICIAL INTELLIGENCE 'MAY REPLACE HUMANS ALTOGETHER'**

### **HUMAN VS AI** How will the Artificial intelligence replace workers?





**Sentinel**One<sup>®</sup>

### Will AI replace Humans?

This time, the robots really are coming.

### Will Robots Replace Humans?



© 2023 SentinelOne. All Rights Reserved.

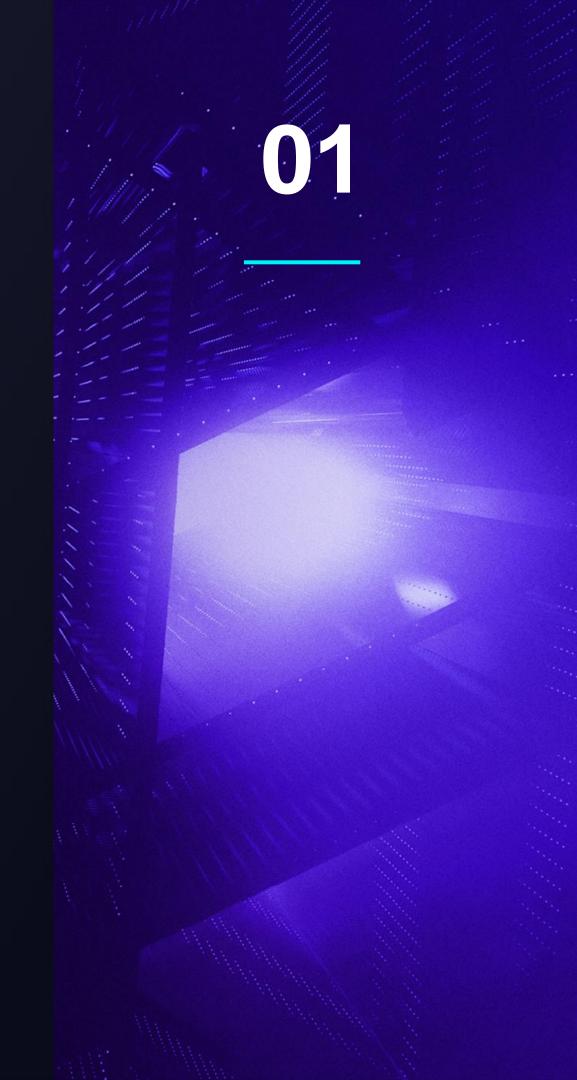


### Or Will Humans and Machines Create Greater Value Together?





### **Cybersecurity Challenges**



### Complexity is the Enemy Of Security

- Anytime, Anywhere Computing
- Cloud PaaS, SaaS, laaS and FaaS
- Application Proliferation
- Pervasive Digitization
- Corporate Owned vs BYOD
- Endless Data Feeds

**Sentinel**One<sup>®</sup>





### **Challenges We Hear From Customers**

### $( \underbrace{0})$

#### Rapidly Expanding Attack Surfaces

Stealthy, advanced threats that continue to evade even the best defenses



#### Complex Multi-Vendor Security Stack

Increasing level of complexity as vendor footprint expands without integrated workflows



#### Manual Triage & Investigation

Disconnected, alertcentric tools with alerts that lack context and correlation



### 

#### Cybersecurity Skills Shortage

Lack of skilled SecOps practitioners with insufficient domain expertise



#### Reactive Processes & Flows

Manual orchestration of responses that happen at individual control points and at human speed

### 10+ Vendors

### **25-49** Tools





© 2023 SentinelOne. All Rights Reserved.

## 57%

Customers claiming to be impacted by skills shortage

### The Quest for Optimized Security Operations

#### Single Pane of Glass...

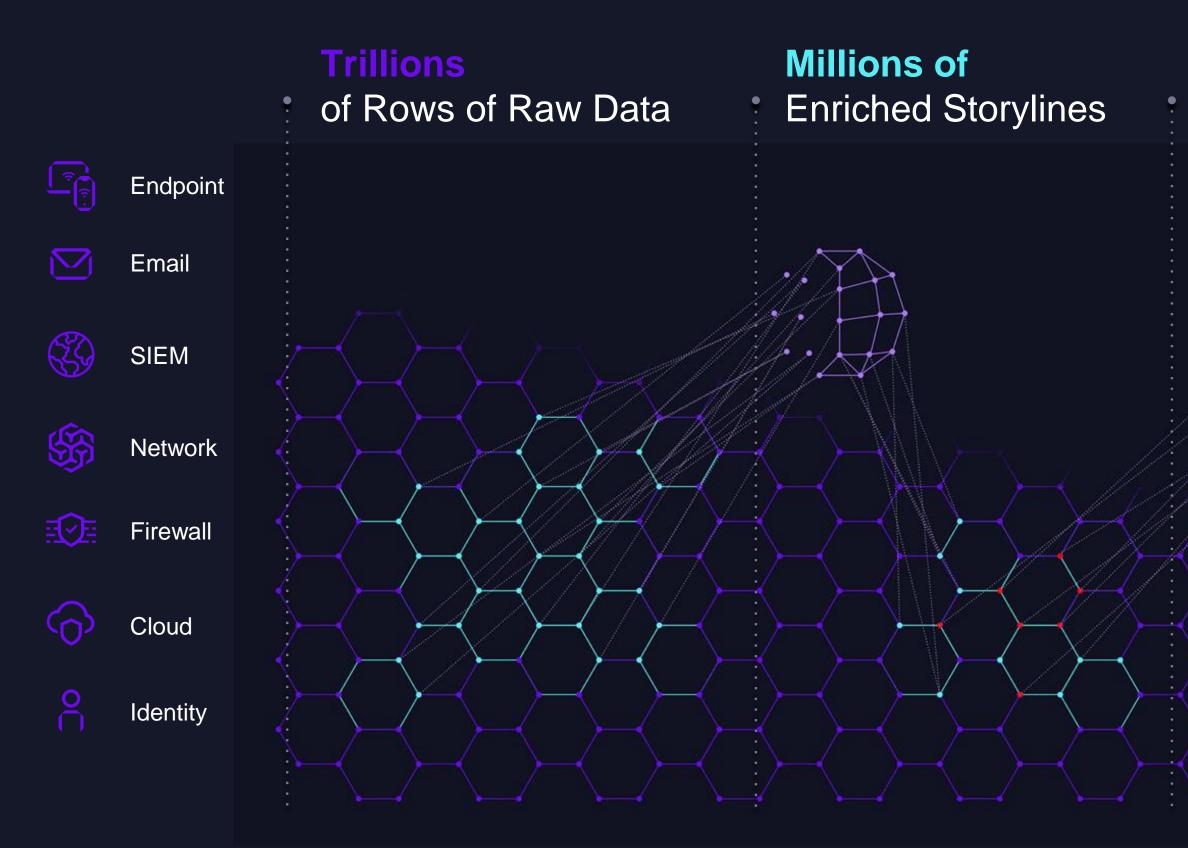
Image: Societa/Methical			٢		ge de la la			
	- U -		Analyst Verdict: True Positive v Ind	Ident Status: Unresolved v				
	Processes •		ſ	tion cmd.exe flodhelper +				
Showing all events for the current threat Al 13, 2021 150026 Ohief Officer Ohief@Krester.com User login to Oka Storage @ AlLOW Rio de Janeiro Rio de Janeiro Roal 45.133.180.134 Fale Al 5, 2021 150026 Ohief Officer Ohief@Krester.com User login to Oka Storage R Stock Stock Rio de Janeiro Ri	Process      Pid      Date        WINWORD.EXE L.      6664      Jul 15, 2021 15:00:01        WINWORD.EXE L.      7008      Jul 15, 2021 15:00:01        rad94987.tmp.exe      420      Jul 15, 2021 15:00:10        cmd are (whaami      6610      Jul 15, 2021 15:01:41        whaami.eme      2772      Jul 15, 2021 15:01:41        whaami.eme      1000      Jul 15, 2021 15:01:42        cmd.exe (whaami      2976      Jul 15, 2021 15:01:43	WINWORD.DXE	WINWORD.EXE (in_	Condesse (whoami.e. Everse 2				
A I Crents    100    Processes    100    Processes    100    Cloud Storage    100	57647		PR04	CESS TREE TIMELINE				
Jul 15, 2021 15:03 26    Chief Officer    Chief@fOrrester.com    Evaluation of sign- on policy    ALLOW    Rio de Janeiro    Rio de Janeiro    Brazil    45.133.180.134    False      Jul 15, 2021 15:03 26    Chief Officer    Chief@fOrrester.com    User login to Okta    SUCCESS    Rio de Janeiro    Brazil    45.133.180.134    False      Jul 15, 2021 15:03 26    Chief Officer    Chief@fOrrester.com    User login to Okta    SUCCESS    Rio de Janeiro    Brazil    45.133.180.134    False      Jul 15, 2021 15:03 26    Chief Officer    Chief@fOrrester.com    User login to Okta    SUCCESS    Rio de Janeiro    Brazil    45.133.180.134    False	Showing all events for the current threat        All Events      1.10* <u>D</u> Files <del>D</del> Network Actions <del>O</del> Processes <u>42</u>	Indicators 338 Cloud Storage 12	ty 10 Email 5.232					
Jul 15, 2021 15:03.26      Chief Officer      Chief@fOrrester.com      User login to Okta      SUCCESS      Rio de Janeiro      Brazil      45.133.180.134      False        Jul 15, 2021 15:03.26      Chief Officer      Chief@fOrrester.com      User login to Okta      SUCCESS      Rio de Janeiro      Brazil      45.133.180.134      False	Timestamp : Username : Email	I Action	E   Result E   City	I   State I   Country	IP Address	1   Threat D 1		
Jul 15, 2021 15:03:26 Chief Officer Chief@f0rrester.com User login to Okta SUCCESS Rio de Janeiro Brazil 45:133:180.134 False	Jul 15, 2021 15:03:26 Chief Officer Chief@f0rrester.com	Evaluation of sign-on policy	ALLOW Rio de Janeiro	Rio de Janeiro Brazil	45.133.180.134	False		
	Jul 15, 2021 15:03:26 Chief Officer Chief@f0rrester.com	User login to Okta	SUCCESS Rio de Janeiro	Rio de Janeiro Brazil	45.133.180.134	False		
Jul 15, 2021 14-58-49 Chief Officer Chief@f0rrester.com User single sign on to app SUCCESS Yukon Oklahoma United States 108.76.207.50	Jul 15, 2021 15:03:26 Chief Officer Chief@f0rrester.com	User login to Okta	SUCCESS Rio de Janeiro	Rio de Janeiro Brazil	45.133.180.134	False		
	Jul 15, 2021 14:58:49 Chief Officer Chief@f0rrester.com	User single sign on to app	SUCCESS Yukon	Oklahoma United States	108.76.207.50			
	Charles and the second s			-		Contraction in the		



#### ... or Single Glass of Pain?



### Signal : Noise Reduction is Critical







#### Handful of Actionable **Campaign Level Incidents**

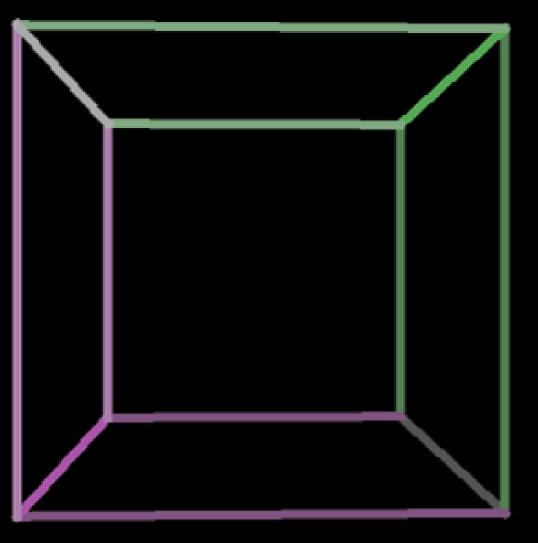


- Accelerate Triage
- **Improve SOC Efficiencies**
- Minimize Dwell Time

### The "Duality" of Black-Box Al

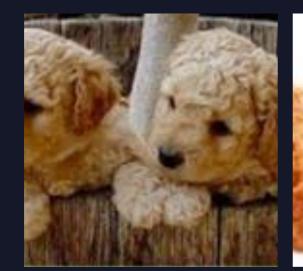
- Non-Deterministic(results may vary)
- Detect Previously Unseen Attacks
- Often Unable to Explain "Rationale" for Conclusion
- False Positives and False
  Negatives are Inherent





#### **Accuracy & Explainability?**

# Can Al Tell the Difference?











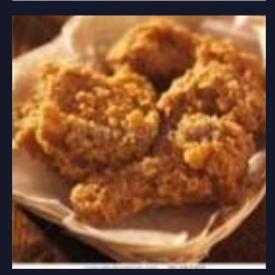


© 2021 SentinelOne. All Rights Reserved























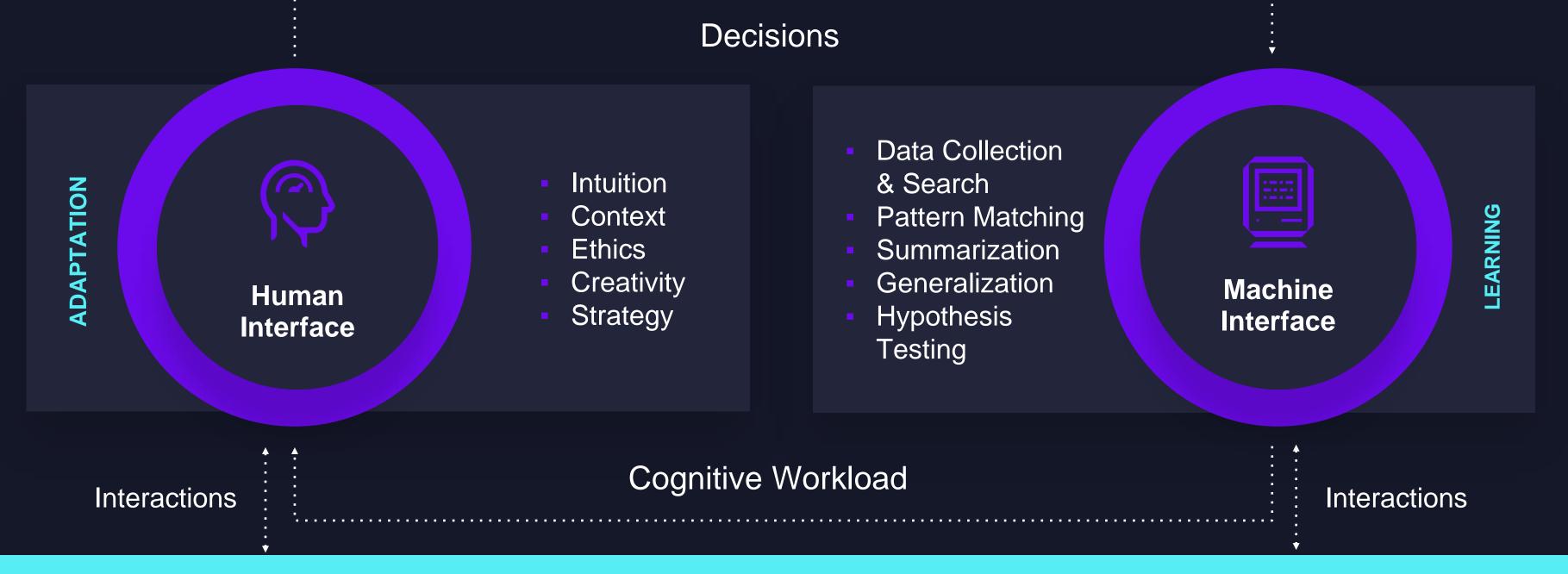


# Are You Equally Comfortable with 90% Accuracy in This Scenario?



© 2023 SentinelOne. All Rights Reserved.

### A Time & Place for Machines



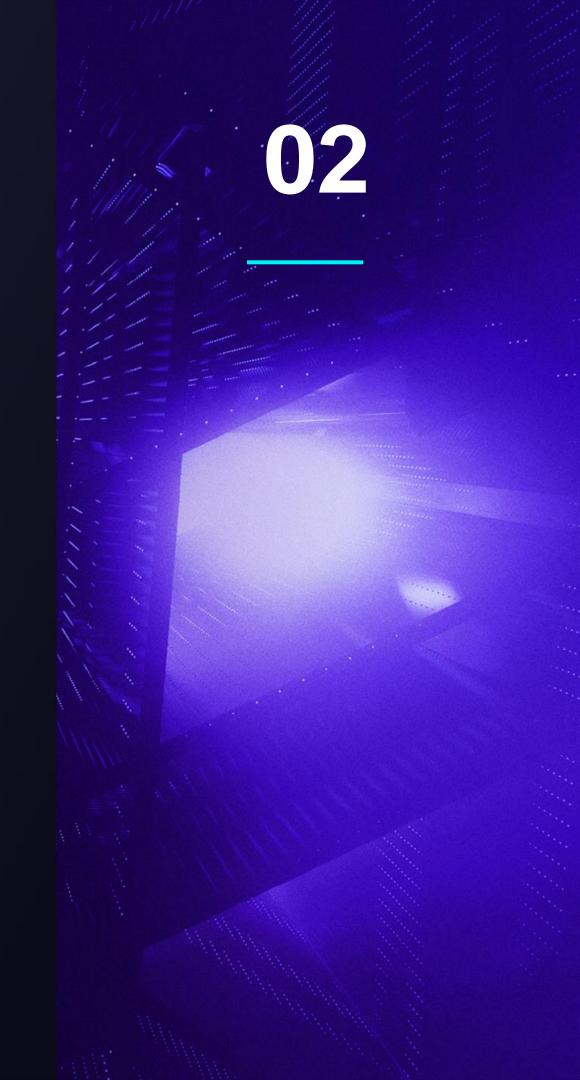
#### "Real" World



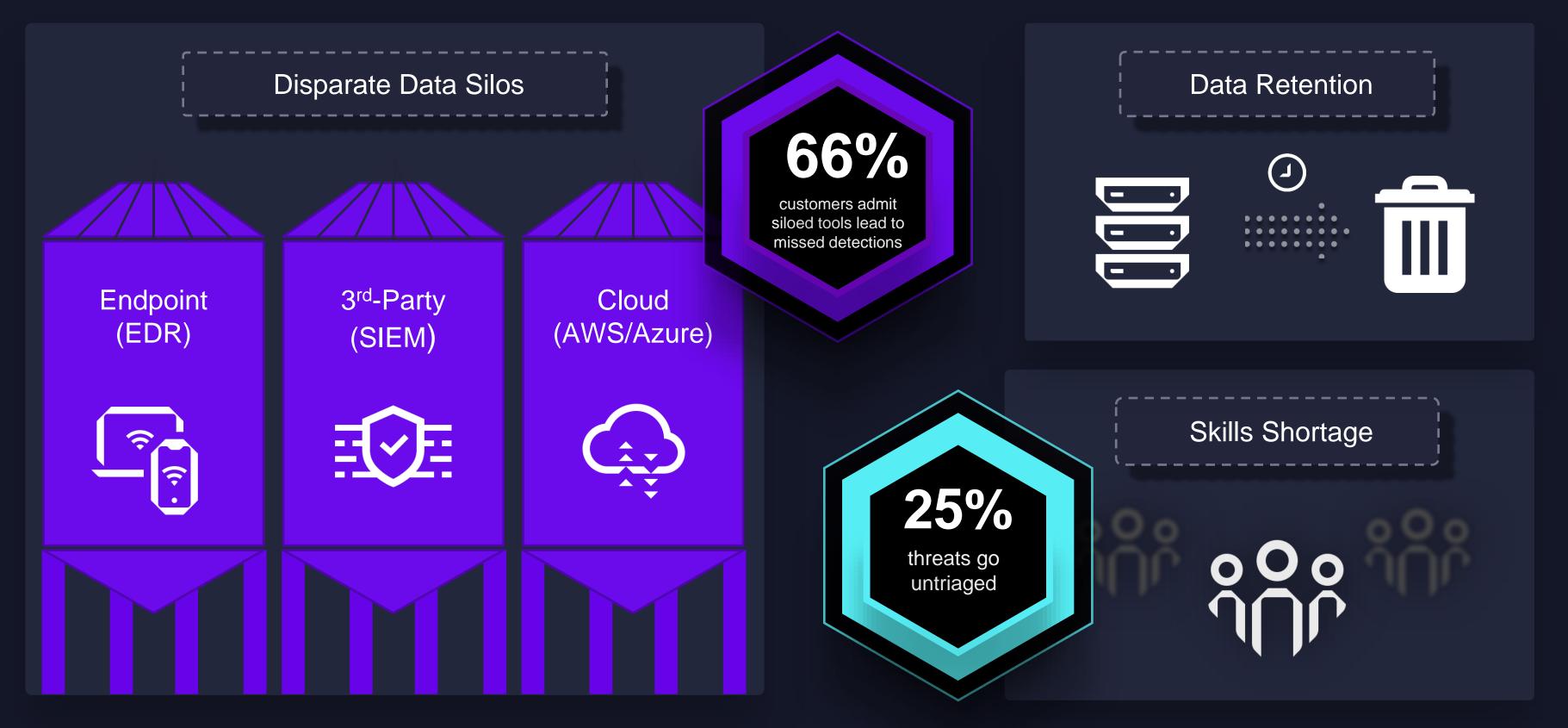
© 2023 SentinelOne. All Rights Reserved.



### SOC as a Proofpoint



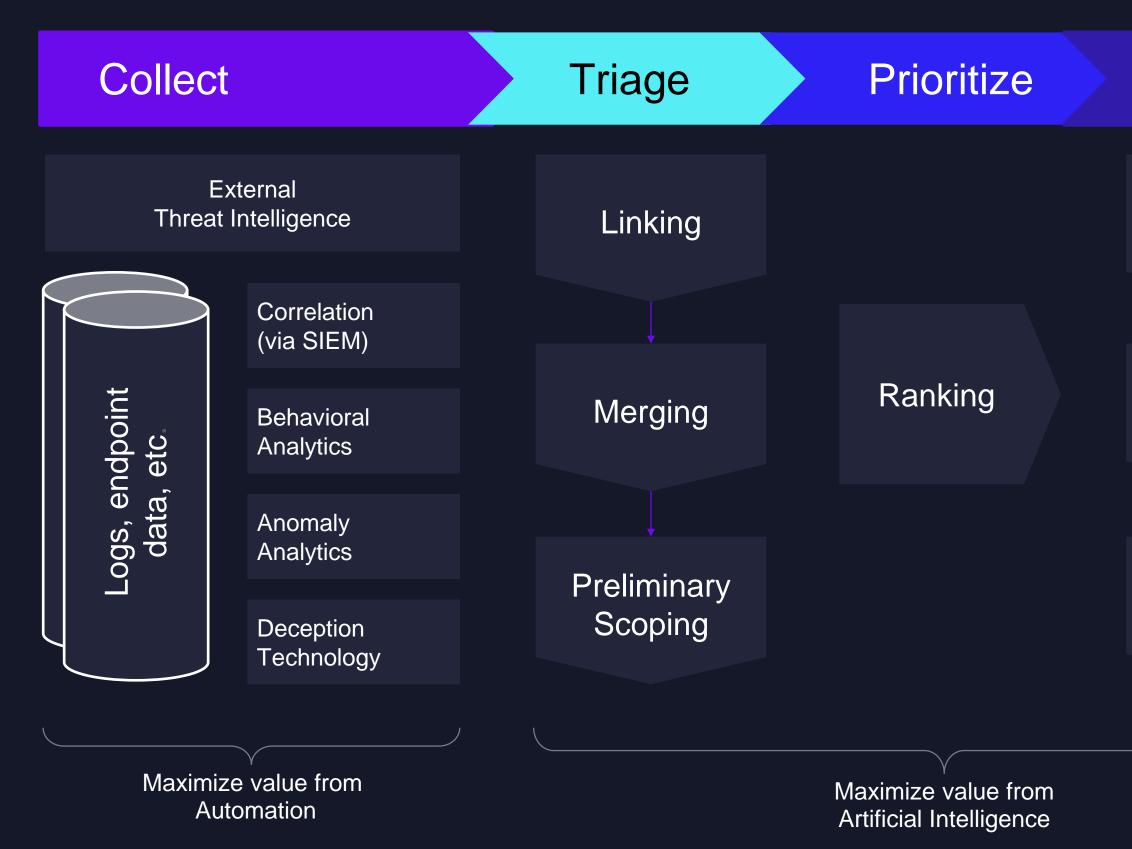
### **Challenges Facing Today's SOC**





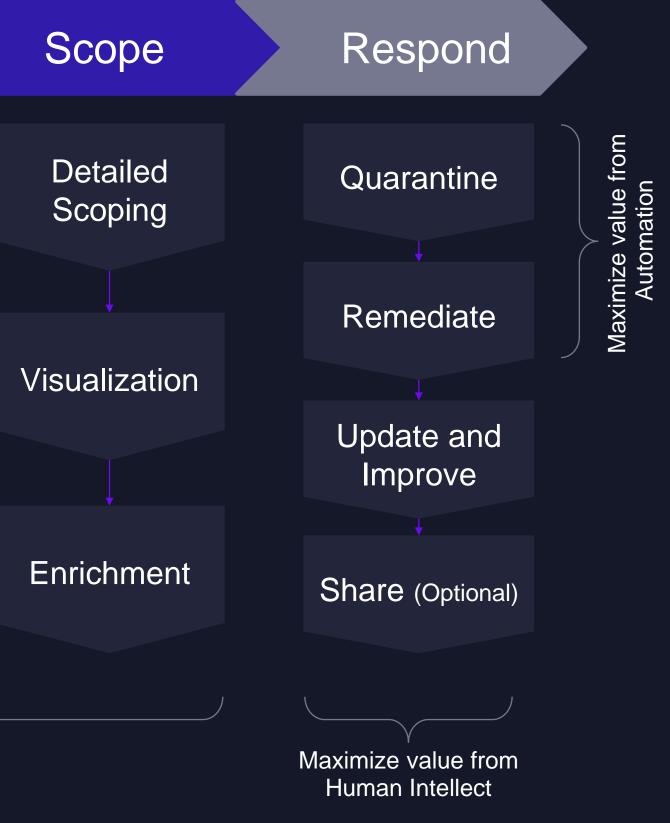


### Workflow of an Attack Investigation





© 2023 SentinelOne. All Rights Reserved.





### Introducing

# PurpleAl

C Page 1 h **inaukor** 

Partness or which

Industri Nor

Ballohergeri

Statistics in the local division of the

Same Streets

from from

Sec. 1

0	ingen gindere	el sentire	-	WE Surry Treamlin				and A 10	4
					Coupe States				
() Di	in the	- 1	ngille in	Qualifier da v	Har Continue Rela	n Alaria	Data +		

#### Antibeing targeted by Securit/Consister 7 Life Transform

Which the entry water's rise for the

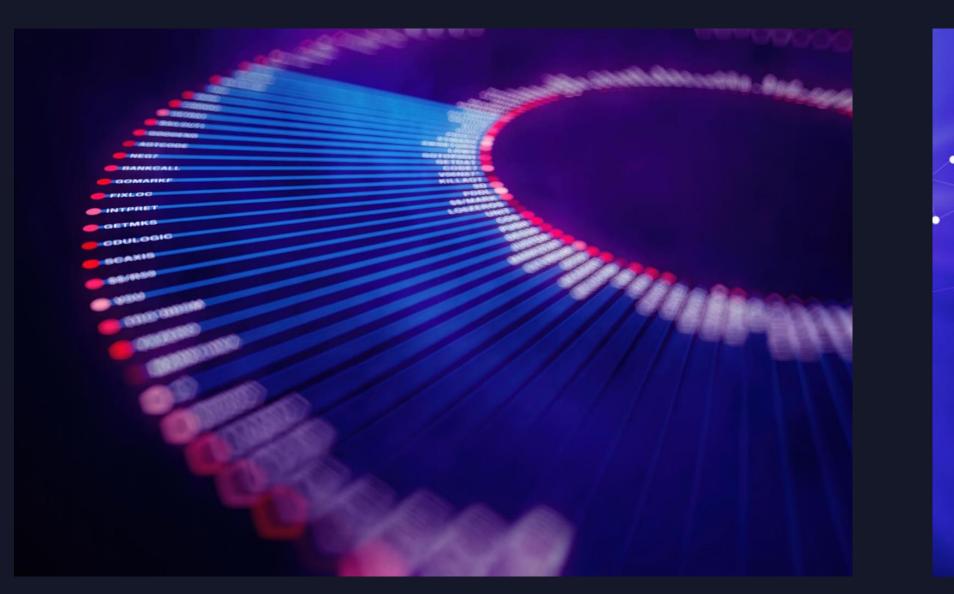
#### In the any Smooth Chevralize activity in my environment 1

and a second part of a second part of any lattice of any lattice of a second part of the p

Saurus Anusea Disription 20	Manipul, Indicator, mark constant, Spectrage
SNREW/WOMEN'	tite age 10 - 2 million de pe
01403478(200847	T April 10 - Antoine And pa
100000000000	In the International State
	t an a constant a
-	25 Apr 18 - 210246-366 pt

### The Whole Is Greater Than The Sum Of Its Parts

#### **Complex Data Analysis**





© 2023 SentinelOne. All Rights Reserved.

#### **Human Intellectual Capital**



### Thank You



#### sentinelone.com

# **Sentinel**One<sup>®</sup>

