Improving Threat Intelligence, Detection, and Response for Cloud Workloads

Dan Constantino

Director, Security Operations

Cox Automotive

Improving Threat Intelligence, Detection, and Response for Cloud Workloads

COX AUTOMOTIVE™

Dan Constantino
Director, Security Operations

Here’s the brutal truth:

Threat actors don’t break in, they log in or exploit old vulnerabilities/misconfigurations

and

Cloud environments can widen the scope of a company’s risk

No exceptions

COX AUTOMOTIVE™

COX AUTOMOTIVE™

INTERNATIONAL

INVENTORY SOLUTIONS

Manheim

RMS/AUTOMOTIVE

RETAIL SOLUTIONS

Autotrader

Dealertrack

Kelley Blue Book

HOMENET AUTOMOTIVE

VinSolutions
Make every connection count.

DEALER.COM

xtime

vAuto
LIVE MARKET VIEW

FINANCIAL SOLUTIONS

NEXTGEAR CAPITAL

MOBILITY SOLUTIONS

CLUTCH

RIDEKLEEN™

FLEXDRIVE

Getaround

RIDECELL

AUTOST. 汽车街 autostreets.com

易车 yiche.com

carsguide

Dealer-Auction.com

DEALER SOLUTIONS

精真估 jingzhengu.com

Mahindra First Choice

Modix

MOLICAR

MOTORS .co.uk

MOVEX

COX AUTOMOTIVE™

IN THE CLOUD

Customer-Facing Systems
(IaaS/SaaS/PaaS)

Corporate Applications
(SaaS)

QA/ RELEASE
ENGINEER

PII

Threat
INTELLIGENCE
Threat
DETECTION
Threat
RESPONSE

Threat
INTELLIGENCE

Threat
DETECTION

Threat
RESPONSE

THR ELLIGENCE

intel
better
ur threats

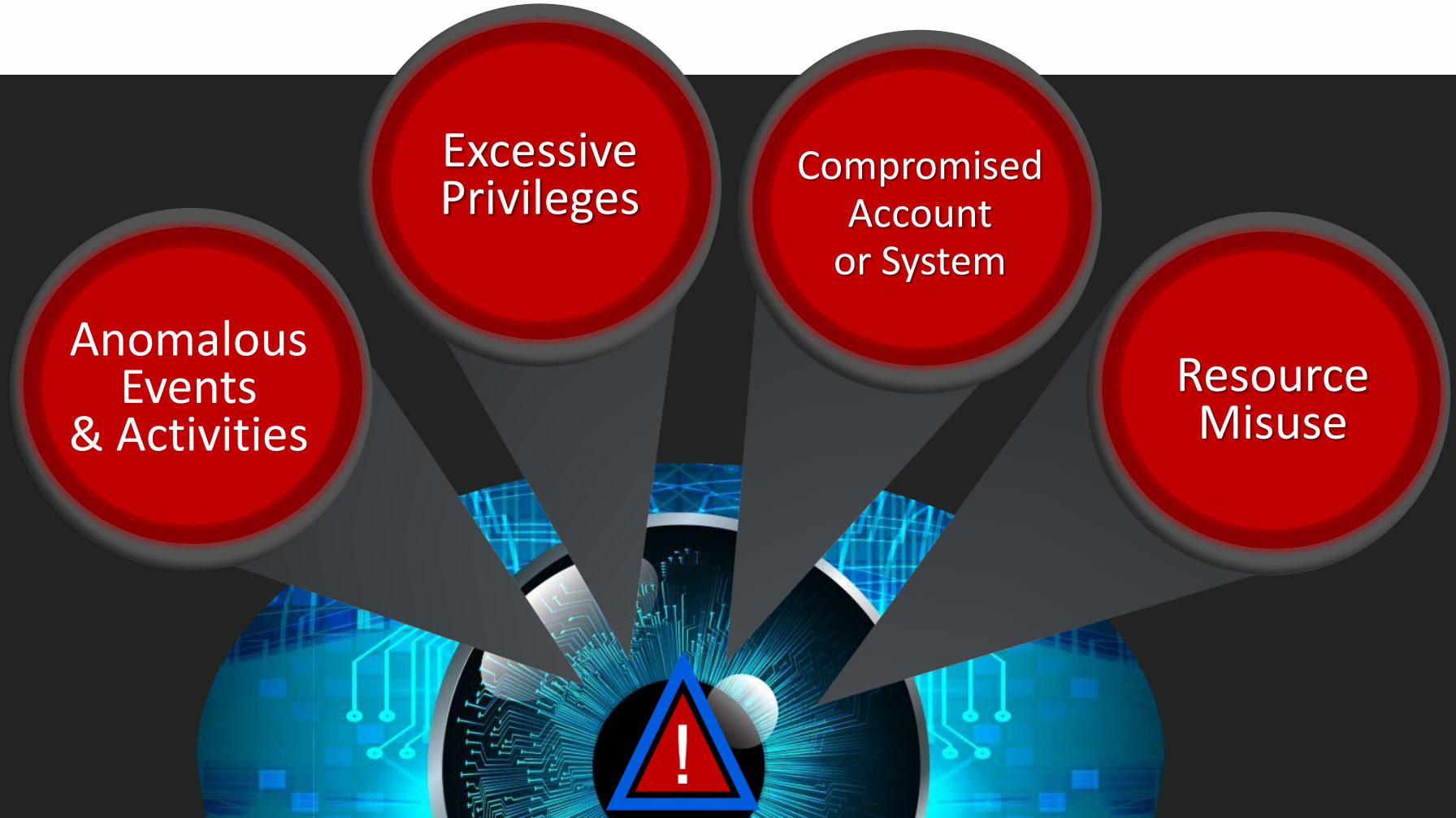
TIPS

- your own threat intel
- Integrate on-prem and cloud threat intelligence within a single platform
- Age out/expire threat intel
- Use your IR artifacts/findings
- Automate 2-way integration of threat intel
- Leverage your threat intel to prioritize vulnerability remediation

THR TION

Threat DETECTION

detection capabilities to identify
and established self-service
v-level threat alerts



THR ONSE

Any/Any
Security Group

Phishing Auto Response - Account password was reset

To Security Monitoring & Response

rules.txt
278 bytes

trace_3days.csv
308 bytes

This is message is a system-generated notification to confirm that the password for account Ellie Phant has been revoked and the corresponding session revoked. Please contact the user and assist them with recovering and checking their account. A message trace for the last 3 days and the current inbox forwarding and delete rules are attached.

OPERATIONALIZE

KEY TAKEAWAYS

- Fully understand your cloud risks and threats
- Create your own threat intel ecosystem
- Set up accurate and actionable alerting
- Automate response for commodity-based threats
- Build a playbook with your use cases

THANK YOU

COX AUTOMOTIVE™

Dan Constantino
Director, Security Operations

CSO50 CONFERENCE+AWARDS

FROM IDG

Innovation Stories from Security Leaders

Vulnerability Management:
Q&A Panel Discussion

Jason Cathey
CISO
Bank OZK

Dan Constantino
Director,
Security Operations
Cox Automotive

Todd Therrien
Interim CISO
City of Phoenix

Moderator: Bob Bragdon, Publisher, CSO