

RSA[®]Conference2017

San Francisco | February 13–17 | Moscone Center

SESSION ID: AIR – T09F

POWER OF
OPPORTUNITY

Sizzle or Fizzle: Is Threat Intelligence Really Worth My Time?

MODERATOR: **Dr. Anton Chuvakin**

Research Vice President at Gartner
@anton_chuvakin

PANELISTS: **Brian Engle**

Executive Director
R-CISC
@brianaengle

Sean McBride

Attack Synthesis Lead
FireEye

David Meltzer

Chief Research Officer,
Tripwire
@davidjmeltzer

Top Threat Intelligence Questions

1. Can we please clearly define threat intelligence (TI), one last time?
2. How to operationalize threat intelligence at different maturity levels of security operations?
3. What types of threat intel has the most value for organizations at different maturity levels?
4. How do you understand the threat intelligence process?
5. What organization resources are needed to make use of TI?

Moderator

Dr. Anton Chuvakin

@anton_chuvakin

Dr. Anton Chuvakin is a Research VP at Gartner for Technical Professionals (GTP), covering topics like security monitoring, threat intel, incident response and others. He is a recognized security expert in the field of SIEM, log management and PCI DSS compliance. He is an author of books "Security Warrior," "PCI Compliance," "Logging and Log Management" and a contributor to "Know Your Enemy II," "Information Security Management Handbook" and others.

Sean McBride

In 2009 Sean co-founded Critical Intelligence to help organizations that own and operate electric generating stations, oil refineries, and water plants understand threats to the industrial processes they operate. His company was acquired by iSIGHT Partners in 2016. He now leads the Attack Synthesis Team within FireEye iSIGHT Intelligence.

Panelists

Brian Engle

@brianaengle

Brian Engle serves as the Executive Director of the Retail Cyber Intelligence Sharing Center (R-CISC), leading the organization from its inception to current state as the trusted resource for cybersecurity information sharing and intelligence for risk and fraud mitigation. The growing R-CISC community brings together consumer facing organizations in the retail and consumer products, goods and services industries.

Panelists

David Meltzer

@brianaengle

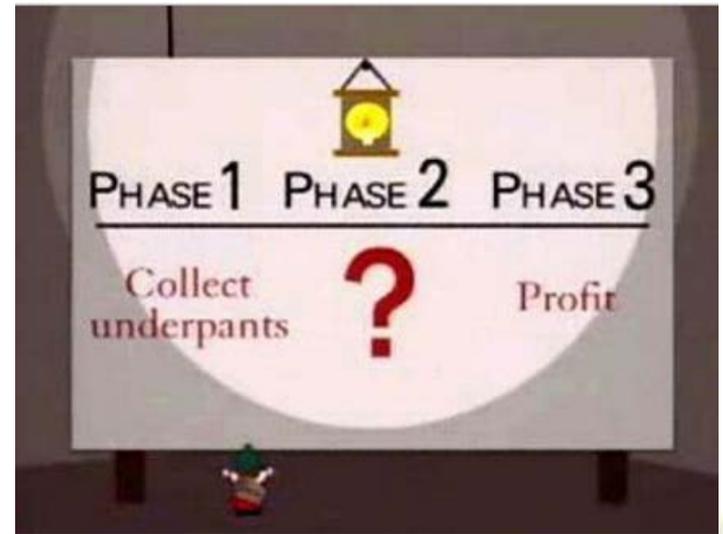
David Meltzer is a security industry pioneer bringing a unique blend of technical expertise, entrepreneurial skill and market vision to his current position as Tripwire's Chief Technology Officer and Vice President of Corporate Development. Meltzer joined Tripwire through its acquisition of nCircle, where he served as Chief Technology Officer and Vice President of Engineering. Immediately prior to joining nCircle, Meltzer was Founder and Chief Technology Officer at Cambia Security, where he pioneered the industry's first agentless configuration compliance auditing solution.

Top Threat Intelligence Questions

1. Can we please clearly define threat intelligence (TI), one last time?
2. How to operationalize threat intelligence at different maturity levels of security operations?
3. What types of threat intel has the most value for organizations at different maturity levels?
4. How do you understand the threat intelligence process?
5. What organization resources are needed to make use of TI?

Still A Common Challenge

1. Get LOTS of threat intelligence
2. ???
3. Profit!



Moderator

Dr. Anton Chuvakin

@anton_chuvakin

Dr. Anton Chuvakin is a Research VP at Gartner for Technical Professionals (GTP), covering topics like security monitoring, threat intel, incident response and others. He is a recognized security expert in the field of SIEM, log management and PCI DSS compliance. He is an author of books "Security Warrior," "PCI Compliance," "Logging and Log Management" and a contributor to "Know Your Enemy II," "Information Security Management Handbook" and others.

Sean McBride

In 2009 Sean co-founded Critical Intelligence to help organizations that own and operate electric generating stations, oil refineries, and water plants understand threats to the industrial processes they operate. His company was acquired by iSIGHT Partners in 2016. He now leads the Attack Synthesis Team within FireEye iSIGHT Intelligence.

Panelists

Brian Engle

@brianaengle

Brian Engle serves as the Executive Director of the Retail Cyber Intelligence Sharing Center (R-CISC), leading the organization from its inception to current state as the trusted resource for cybersecurity information sharing and intelligence for risk and fraud mitigation. The growing R-CISC community brings together consumer facing organizations in the retail and consumer products, goods and services industries.

Panelists

David Meltzer

@brianaengle

David Meltzer is a security industry pioneer bringing a unique blend of technical expertise, entrepreneurial skill and market vision to his current position as Tripwire's Chief Technology Officer and Vice President of Corporate Development. Meltzer joined Tripwire through its acquisition of nCircle, where he served as Chief Technology Officer and Vice President of Engineering. Immediately prior to joining nCircle, Meltzer was Founder and Chief Technology Officer at Cambia Security, where he pioneered the industry's first agentless configuration compliance auditing solution.

Apply What You Have Learned Today

#RSAC

- This will be created during the session