SPEAKER: ROB STRICKLAND – CEO of Move 37 Ventures

# *Transforming Security Infrastructure: From Alert Fatigue to Full-Fidelity Defense*

M37 VENTURES

# PERSPECTIVES IN PRACTICE

M37's ecosystem connections, deep technical expertise, and hands-on operational experience enable us to execute bigger, faster, and more effective engagements and deliverables for our clients.

# M37 CLIENT HISTORY

## Advisory & Board

afiniti
SingleStore
Vapor
TRUEFORT
SmarTek21 ACCELERATE YOUR ENTERPRISE
b2b SOFT
RStor
yugabyteDB
DGS
Rady Children's Hospital San Diego
TessPay

## Interim & Executive Leadership

LPL Financial
KYMETA
PERDIX
text+
Televisa
GXC
neustar
infovista

## Ops, Planning, Project & Implementation

globys
epiq
csg INTERNATIONAL
THE WEBSTER
RENEW FINANCIAL
T-Mobile
Private Tech
KPMG
SEMPRE INTEGRITY | SERVICE | INNOVATION

## Biz Dev, Marketing, and Events

AXONIUS
SERAPHIC SECURITY
expeto
GXC
MOTIVE
DELPHIX
CROWN CASTLE
Nametag
Lightspin
SmarTek21 ACCELERATE YOUR ENTERPRISE
DGS
AriaTech controls and more...

## Other Engagements

SOOS
NIR-YU
SINC
CMO CONSULTING
5G OPEN INNOVATION LAB

# SECURITY ARCHITECTURES BUILT FOR YESTERDAY'S THREATS, NOT TODAY'S

- Threat volume soaring (cyber-attacks 30% YoY, ARMIS)
- Detection still lags; Dwell time still > 20 days (Mandiant)
- Cost of breaches high (avg of $4.4M, IBM)
- Salt Typhoon undetected > 1 year
- SEC 4-day disclosure requirement
- Legacy systems can't interrogate full-fidelity data
- Traditional models don't address persistent, sophisticated threats – "unknown unknowns"

M37 VENTURES

# ENHANCED VISIBILITY AND HARDENING GUIDANCE

Published Dec 3, 2024

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
PART OF THE GCSB

https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure

sources / Enhanced Visibility and Hardening Guidance for Communications Infrastructure

PUBLICATION

## Enhanced Visibility and Hardening Guidance for Communications Infrastructure

**Publish Date:** December 04, 2024

**RELATED TOPICS:** CYBERSECURITY BEST PRACTICES, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBER THREATS AND ADVISORIES

### Introduction

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ) warn that People's Republic of China (PRC)-affiliated threat actors compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. The authoring agencies are releasing this guide to highlight this threat and provide network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful exploitation carried out by PRC-affiliated and other malicious cyber actors. Although tailored to network defenders and engineers of communications infrastructure, this guide may also apply to organizations with on-premises enterprise equipment. The authoring agencies encourage telecommunications and other critical infrastructure organizations to apply the best practices in this guide.

As of this release date, identified exploitations or compromises associated with these threat actors' activity align with existing weaknesses associated with victim infrastructure; no novel activity has been observed. Patching vulnerable devices and services, as well as generally securing environments, will reduce opportunities for intrusion and mitigate the actors' activity.

M37 VENTURES

# *THE SECURITY GAP: INCOMPLETE DATA*

More tools ≠ better protection — high-quality, complete data is the key.

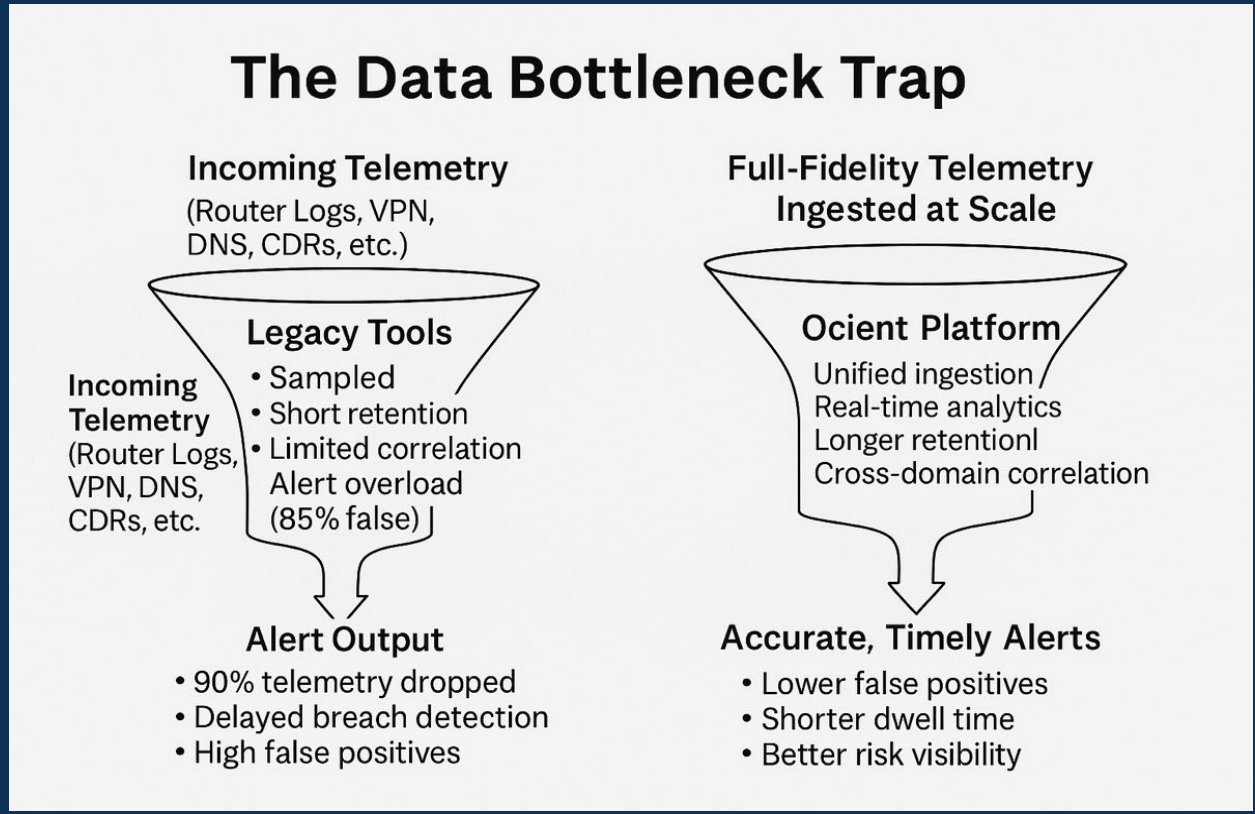
- Legacy SIEMs generate thousands of alerts daily
  - 85% are false positives
  - 78% of CISOs report alert fatigue
  - <10% of telemetry is analyzed
- Result: Blind spots, short retention, and weakened defenses.

Data bottlenecks = risk | Attackers exploit these gaps

vs

No sampling, no compromise.

Modern platforms like Ocient ingest and analyze full-fidelity telemetry at scale




M37 VENTURES

(OCIENT)

# CASE STUDY: GLOBAL CSP

Ocient's Network Intelligence solution enabled our customer to track down multiple bad actors within days

## SITUATION

Urgent need to fulfill stringent compliance SLAs with a large-scale data retention system for comms data.

Preference to deploy on prem with a streamlined solution, CapEx pricing model and low environmental footprint to support carbon reduction goals.

M37 VENTURES

## RESULTS

- > 275 billion network flows per day streaming into the Ocient Data Retention and Disclosure System
- Joint solution and seamless integration with network probe partner
- One year of data accessible in a single rack, a secure on premises environment, with low energy consumption
- 100% of compliance SLAs attained

(OCIENT)

# FASTER – LESS FRICTION – LESS COST – BETTER ARCHITECTURE

LEADING TELCO Customer

5 PB CASE STUDY

OpenSearch elastic

= 5+ racks

100+ Nodes
40TB/node
5+ Racks & DC Floor Tiles

(OCIENT)™

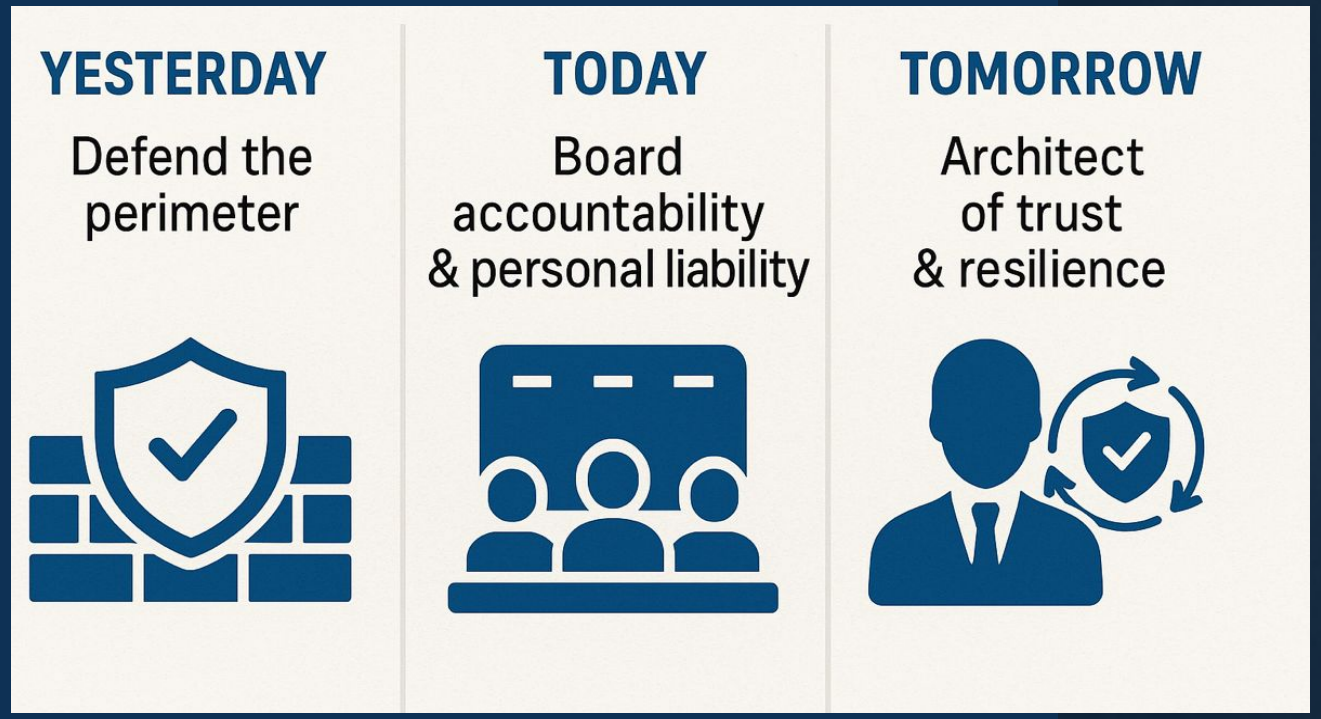
= Single rack

16 Nodes
200TB/node @ 85% compression
*Single rack / data center floor tile*

M37 VENTURES

Ocient.com

# THE CHANGING WORLD OF THE CISO




*"You can't secure what you can't see. Complete visibility and continuous analysis are essential for detecting and responding to threats in real time."* — Gartner, *"Top Trends in Cybersecurity 2023"*

M37 VENTURES

Jeff Simon, CIO, T-Mobile USA

# Q & A

M37 VENTURES

**empowering new ventures, growing businesses, and connecting technology leaders**

www.m37ventures.com

# Questions

1. Is your data infrastructure built for full-fidelity telemetry at modern scale? Are you just sampling and hoping?
2. Where does your team lose the most time during an incident: locating, moving, or querying the data?
3. What % of your security spend drives detection and prevention, not just collection?
4. When was the last time a threat hunt returned answers fast enough to keep your analysts in flow?
5. If you're personally accountable for breaches and reporting, do you own the data infrastructure behind it?

M37 VENTURES

# OCIENT ANALYTICS AT TELEMETRY SCALE

Built to store analyze, and act on trillions of records- at machine speed and scale

## Performance & Scale

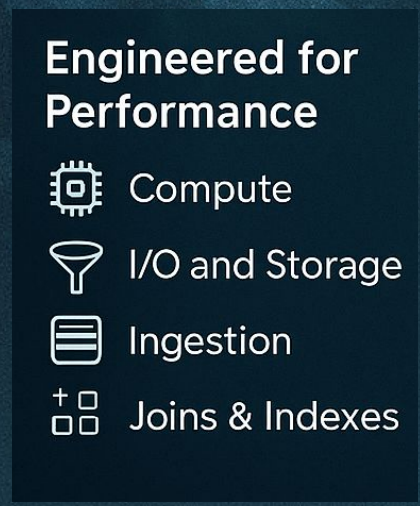
- Ingest up to Tbps
- Hunt, query, and analyze years of data
- Accelerate analytics by 10x to 100x

## Cost & Efficiency

- Extend retention @ 80% less cost
- Use less infrastructure

## Compliance & Visibility

- See every event, not just samples
- Meet SEC breach reporting deadlines







Ocient.com