(ISC)² WEBINARS
SECURITY BRIEFINGS

Is Network Evidence Really Needed for Security Operations?

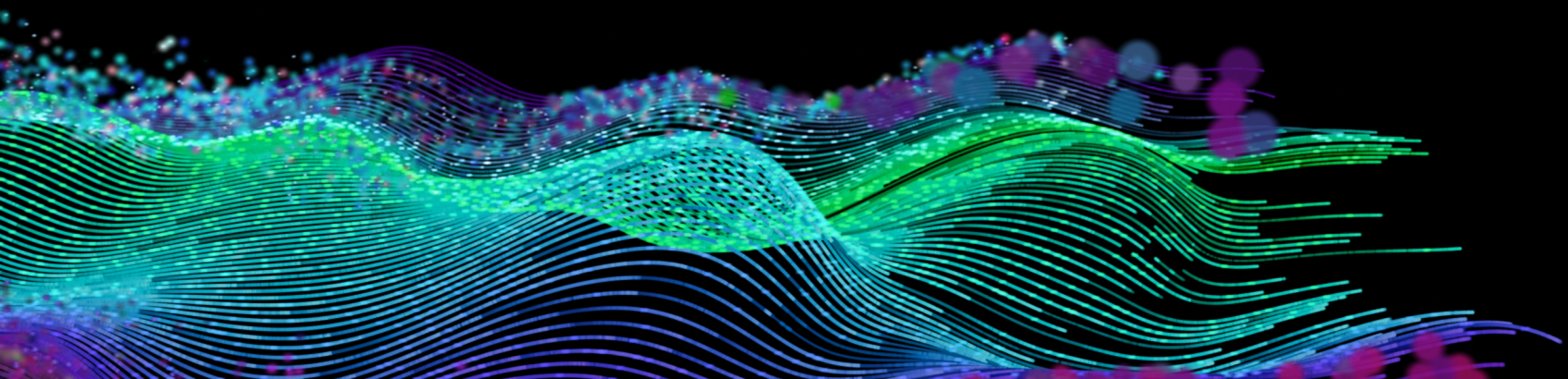
Ashley 'AJ' Nurcombe, Sr Cybersecurity Consultant, Corelight

Brandon Dunlap, Moderator

corelight

corelight

Is Network Evidence Really Needed for Security Operations?



Ashley “AJ” Nurcombe

Senior Cyber Security Consultant - UK&I

TOPICS

- Early days
- Perfect storm
- Our collective dilemma
- Why network evidence continues to matter
- Modernising the ways and means of evidence collection

EARLY DAYS

- Networks were simple
- Client-Server
- Dedicated WAN Links
- Internet with Firewall
- No Wi-Fi, Mobile Devices or IoT

EARLY DAYS

- **The network was easy to study and provided defenders a compelling vantage point**
  - Minimal encryption
  - Transparent communication and simple clear-text protocols
  - Classic tools: Bro (Zeek), Snort, Ethereal (Wireshark)

Perfect Storm

- **Today's networks are significantly more complex**

Nothing stands still

- Encryption is the norm
- Cloud-native apps
- Work from anywhere
- ZT, SASE, SSE
- Unmanaged >> managed

Compounded by

- Digitization of everything
- Powerful attack tools
- lucrative zero-day market
- Politicisation of the Internet
- Rising conflict and risk

Perfect Storm - Greater Complexity & Greater Risk

Does Network Monitoring *still* offer Defenders a Compelling Vantage Point?

Network Evidence is a Critical Element in any Balanced Defensive Strategy

Initial detection
Every vendor failed

LOG4J

Application level vuln initially missed by EDR, IPS/IDS, etc.

solarwinds

Malware concealed itself from EDR, IPS/IDS, etc.

DISCOVERY	Alibaba / Apache Foundation finds vulnerability; cites network as prime discovery recommendation	"Attacker actions had a hard time hiding from all the research done by folks at @corelight_inc." - *Scott Runnels, Mandiant*
DETECTION	Detections available within 24-48 hrs	Detections available within 24-48 hrs
INVESTIGATION	**"With so many exploit paths, what happened to us?"**	**"When was I first affected, and what happened then?"**

Attackers Cannot Easily Avoid Leaving Traces on the Network

We need to think differently about the ways and means of collecting network evidence

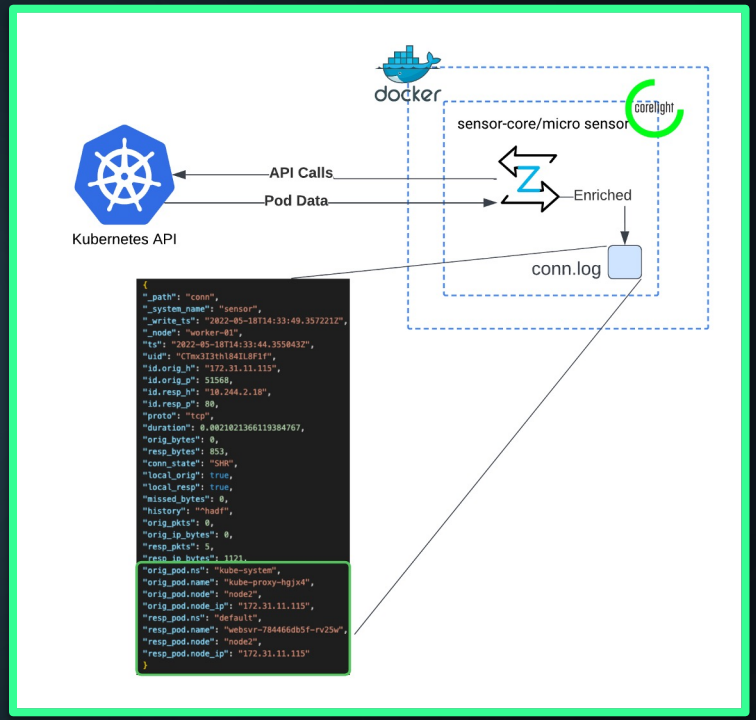
Encrypted Traffic is Filled with Valuable Information

Engineered Visibility

- **Shake the Box!**
  - Encryption creates artifacts
- **Dozens of Inferences**
  - Spacing between packets
  - Sequencing of timestamps
  - Correlation between traffic in one flow and another
  - Human typing or machine interaction
  - Detect DNS over HTTPS or TLS (special algorithm)

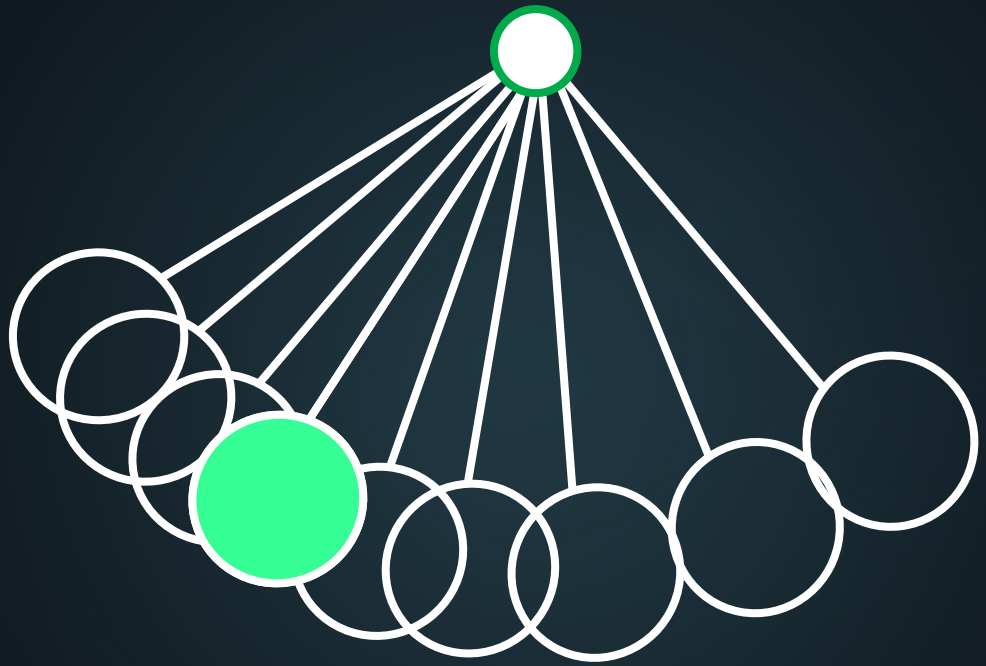
Modern Architectures Present New Opportunities

- Mirroring traffic (eg. CNI, Sidecar)
- Analyzing traffic (w/enriched Zeek logs)
- Generating new insights



The Pendulum is Swinging Back

ENDPOINT



NETWORK

XDR

CROWDSTRIKE corelight

Making it Actionable

- Data quality matters more than ever (NetFlow doesn’t cut it!)
- Encryption is not the end of the road
- New app architectures can provide advantages for collection of network evidence
- SASE / CASB / SSE / ZT can be an opportunity, not an obstacle
- Even the most skilled adversaries leave traces in network traffic

Q&A

corelight