

Trellix

EMEA Security Summit

Barcelona, Spain



Trellix

Striking a Chord with Innovation

Harmonizing XDR, AI,
Threat Intelligence, and
Classic Music Videos



EMEA Field CTO, Trellix



John Fokker

Head of Threat Intelligence, Trellix

Resilience through Innovation



Resilience through Adaption



...Urgently



73%
of Organizations
are scaling AI
investments...
Is there a Risk?

64%
“Use AI in multiple
business functions”

42%
“Customer facing
functions”

31%
“Inside IT
Functions”

Highlight what matters with Trellix Wise



OFFICE 365 [Password Spray]

GenAI ANALYSIS:

Based on the information provided, there are several concerning factors that warrant escalating the severity of this alert:

- The alert description indicates a potential password spray attack was detected from this IP, which is a serious threat.
- The supporting rule hits show suspicious activity like brute force logins, EC2 instances being manually created, and **Tor usage** - all potential signs of compromise.
- The IP was involved in an analytics advisory for data exfiltration, another serious threat.
- The recent Office 365 activity shows **failed logins for an external user**, but also successful logins and inbox rule changes for internal users. This suggests the attacker may have compromised an internal account.

Never miss an alert

Most security staff only look at 10% of their alerts.

Alerts investigated with time available:

(e.g. 5 people * 8 hours = 40 hours/day)

10%

Trellix XDR raises alert scores so analysts see them.

Alerts unseen for AI to investigate:

(Work remaining: 360 hours/day)

Trellix AI

In this example, Trellix AI performs the work of 45 people!



*“Now look at them yo-yos,
that's the way you do it
You play the guitar on the MTV
That ain't workin', that's the way
you do it. Money for nothin'
and your chicks for free”*

– Dire Straits, Money for Nothing



Money for Nothing...

LockBit ransomware gang has over \$110 million in unspent bitcoin



But it does come at a price

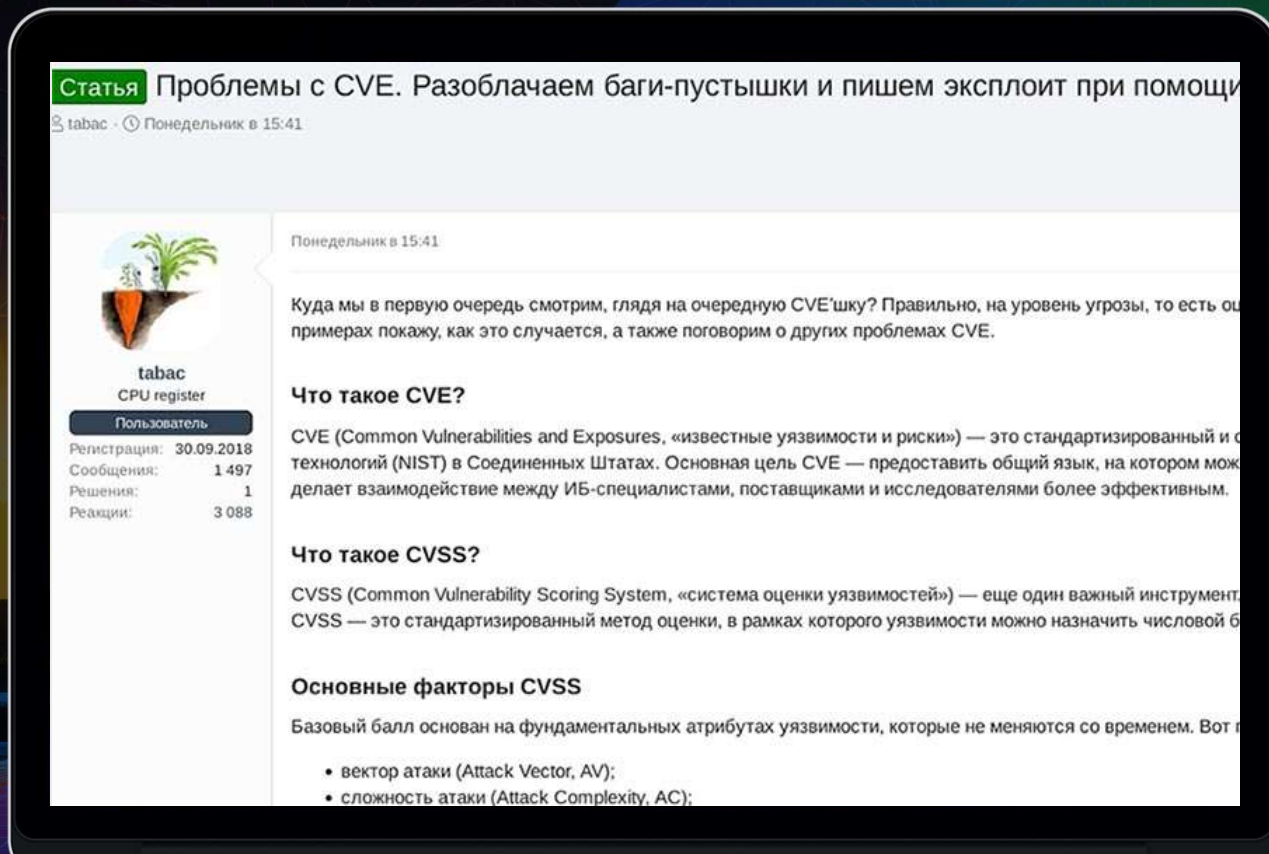
☰ CNN Politics SCOTUS Congress Facts First 2024 Elections

Member of ransomware gang sentenced to more than 13 years in prison over 2021 attack

FBI seized \$2.3M from affiliate of Revil, Gandcrab ransomware gangs

Threat Actors are using AI to...

Code exploits with help of GPT-4 and automate exploitation





Which one is the Real Elon Musk ?



“...Security Strategy Imperatives in the Age of AI ...”

Trellix

Defensive Urgencies

“Think Phishing Defense in Depth, Ransomware Resilience and Insider Risk Management”

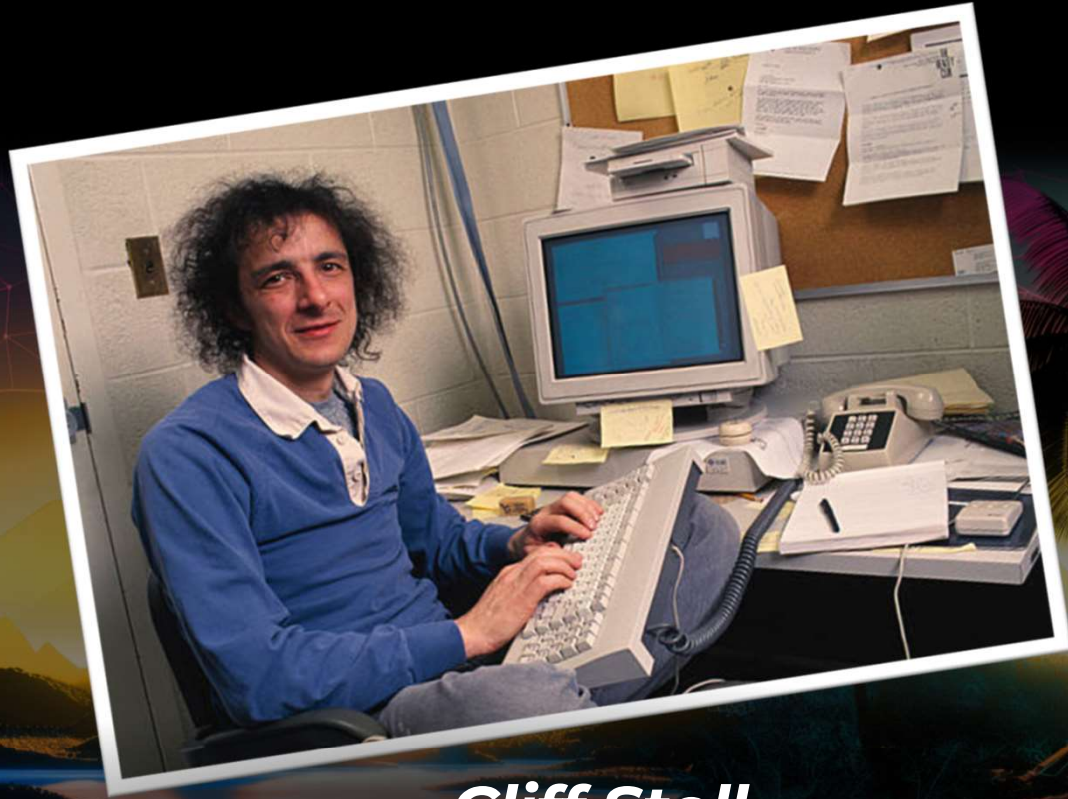
Zero Trust Mindset

“US DoD, CISA, NIST Cyber Risk Management Frameworks”

Sec Ops Evolution

“Modernize your soc with new technology, processes and deep visibility”

Once upon
a time...



Cliff Stoll –

Was the Face of Cyber Security
Incident Response

Adaptive Sec Ops Pillars



Incident
Response



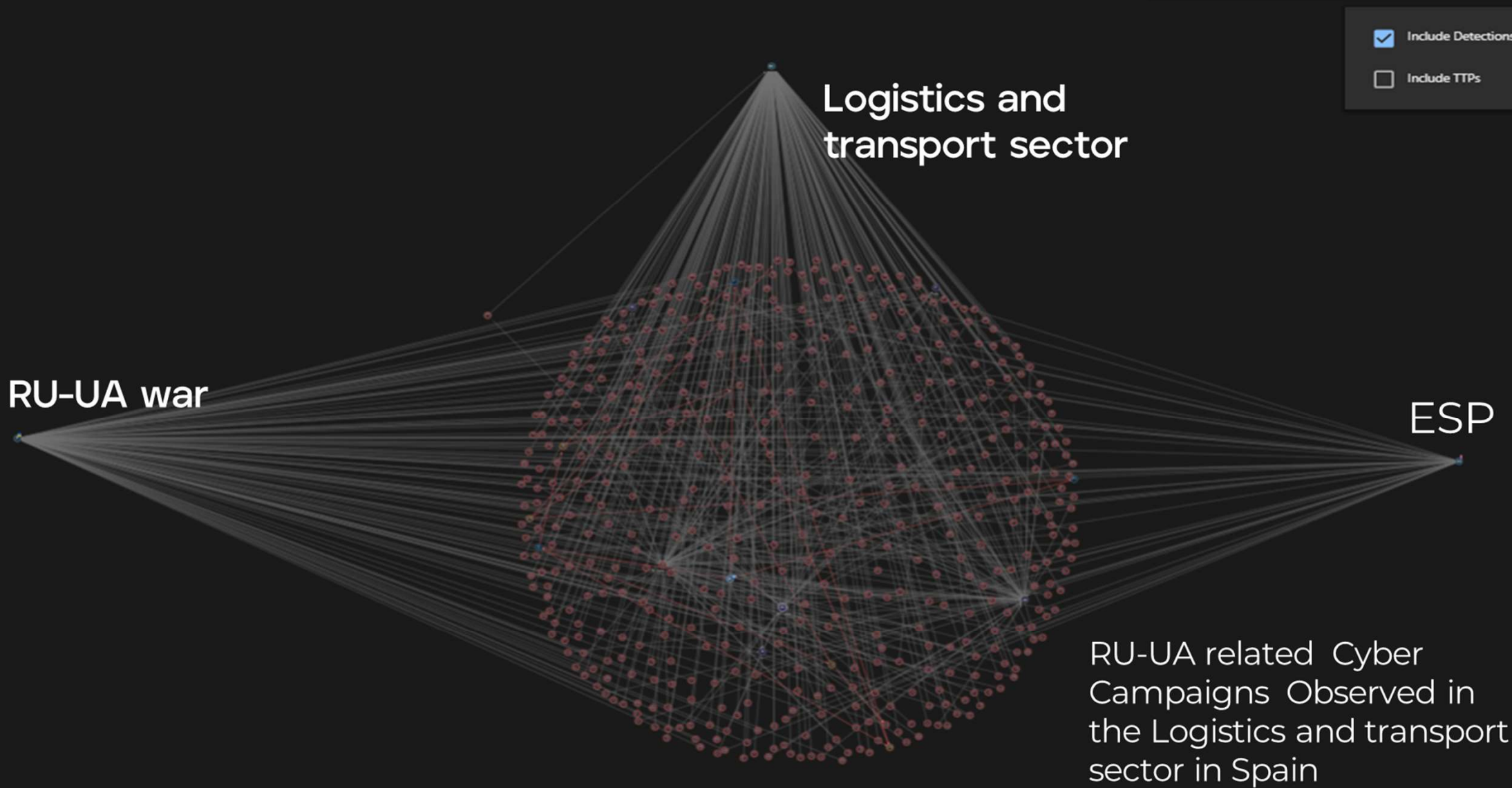
Threat
Hunting



Exposure
Management

Elevate your SOC today...





Theory vs Reality...



SOC 3.0 with Trellix XDR...



SOC 2.0

- Alert Fatigue
- Waste time tuning tools to reduce alerts
- Only investigate alerts that are obvious
- Focus only on Incident Response
- Automation is seperate



SOC 3.0

- Focus on incidents vs events
- Turn on all available alert sources
- Deep investigations on alert clusters
- Time for threat hunting
- Pervasive Hyber Automation

It's time to Come Together

