Trellix

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

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

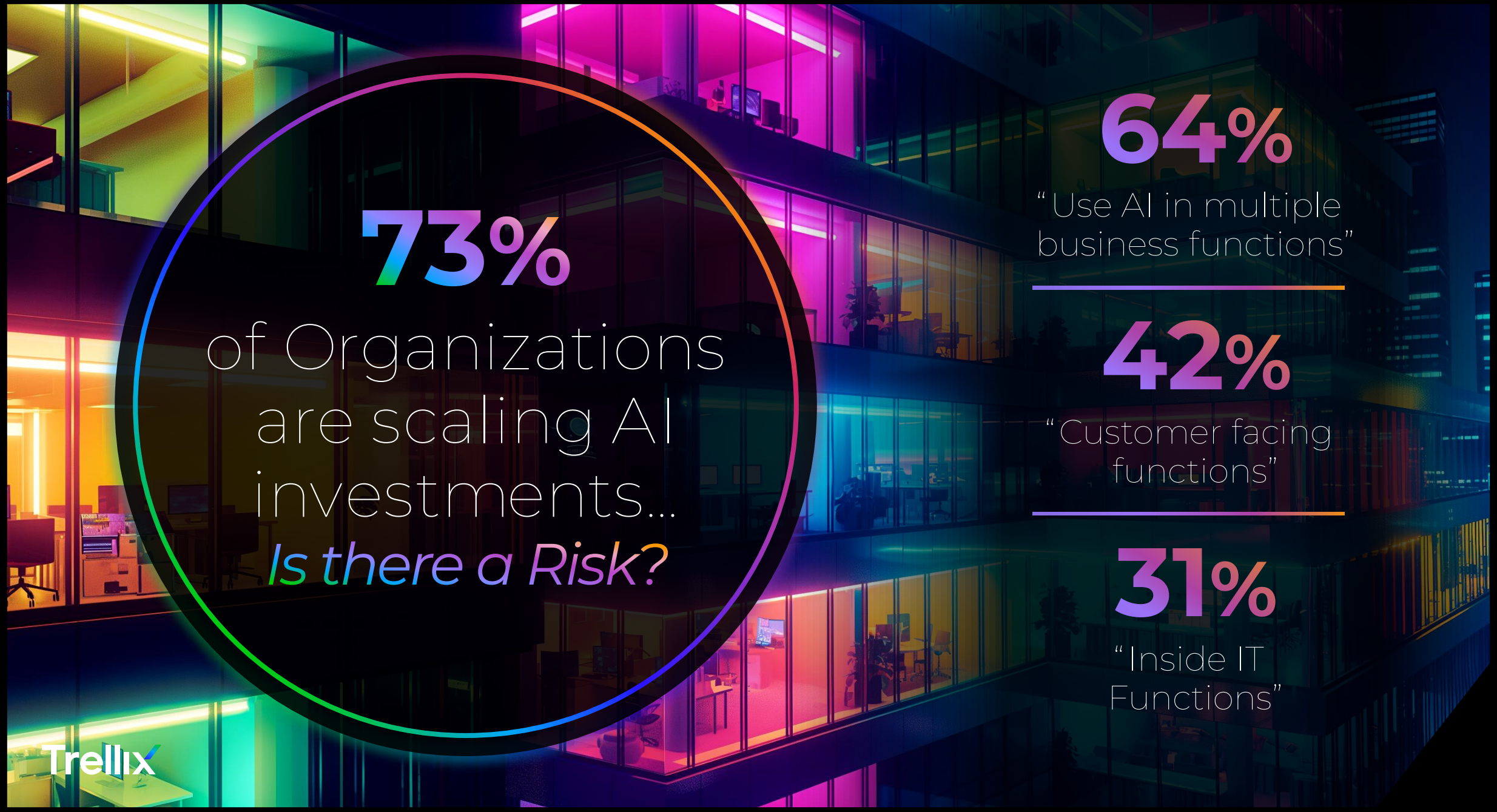
Resilience through Innovation

Trellix

Resilience through Adaption

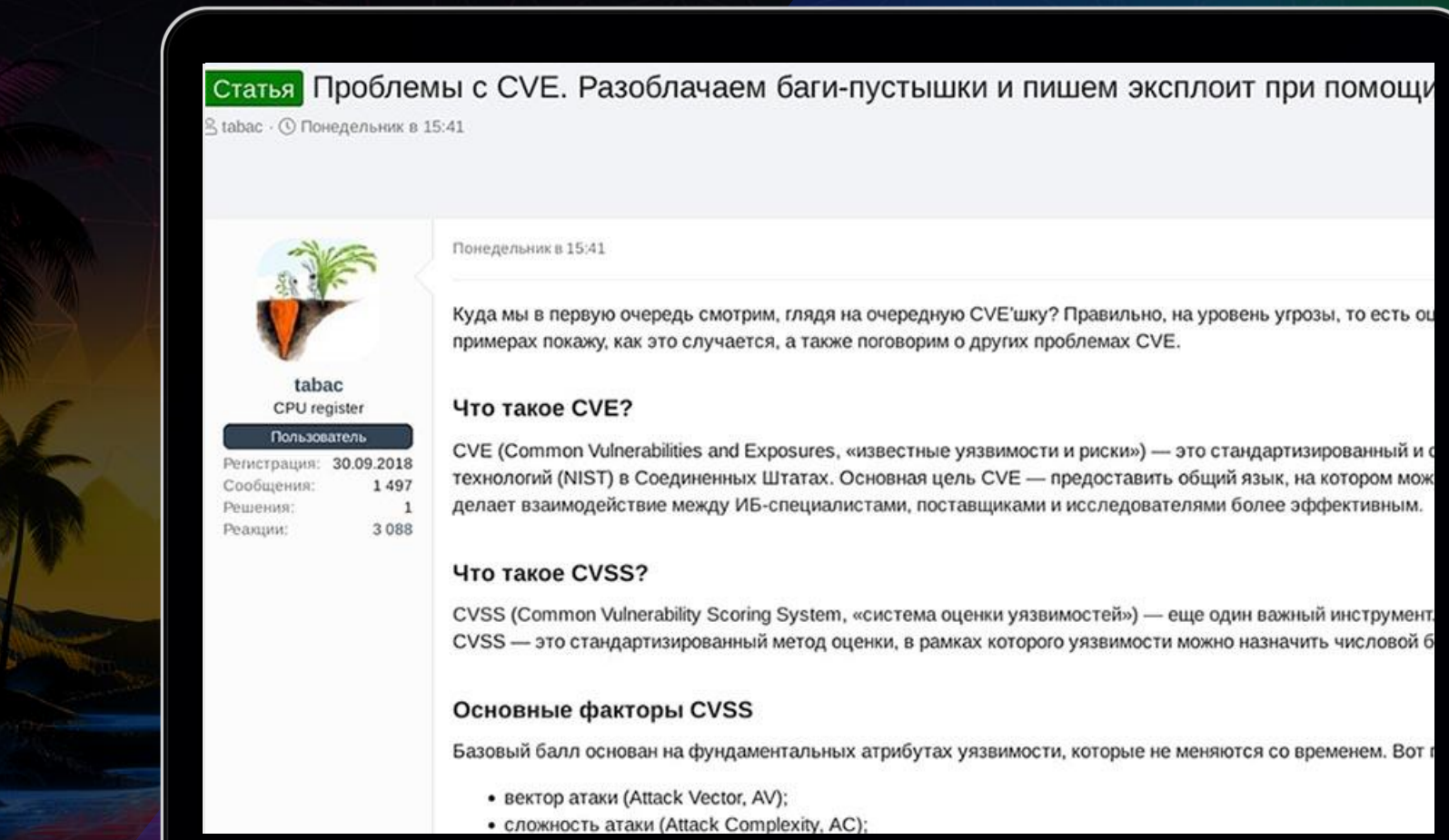
... Urgently

Trellix


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"
Trellix

Threat Actors are using AI to...

Code exploits with help of GPT-4 and automate exploitation



Trellix

https://www.trellix.com/blogs/research/the-dark-side-of-innovation-cybercriminals-and-their-adoption-of-genai/

1

2

Which one is the Real Elon Musk ?

Trellix

https://www.trellix.com/blogs/research/the-dark-side-of-innovation-cybercriminals-and-their-adoption-of-genai/

Highlight what matters with Trellix Wise

OFFICE 365 [Password Spray]

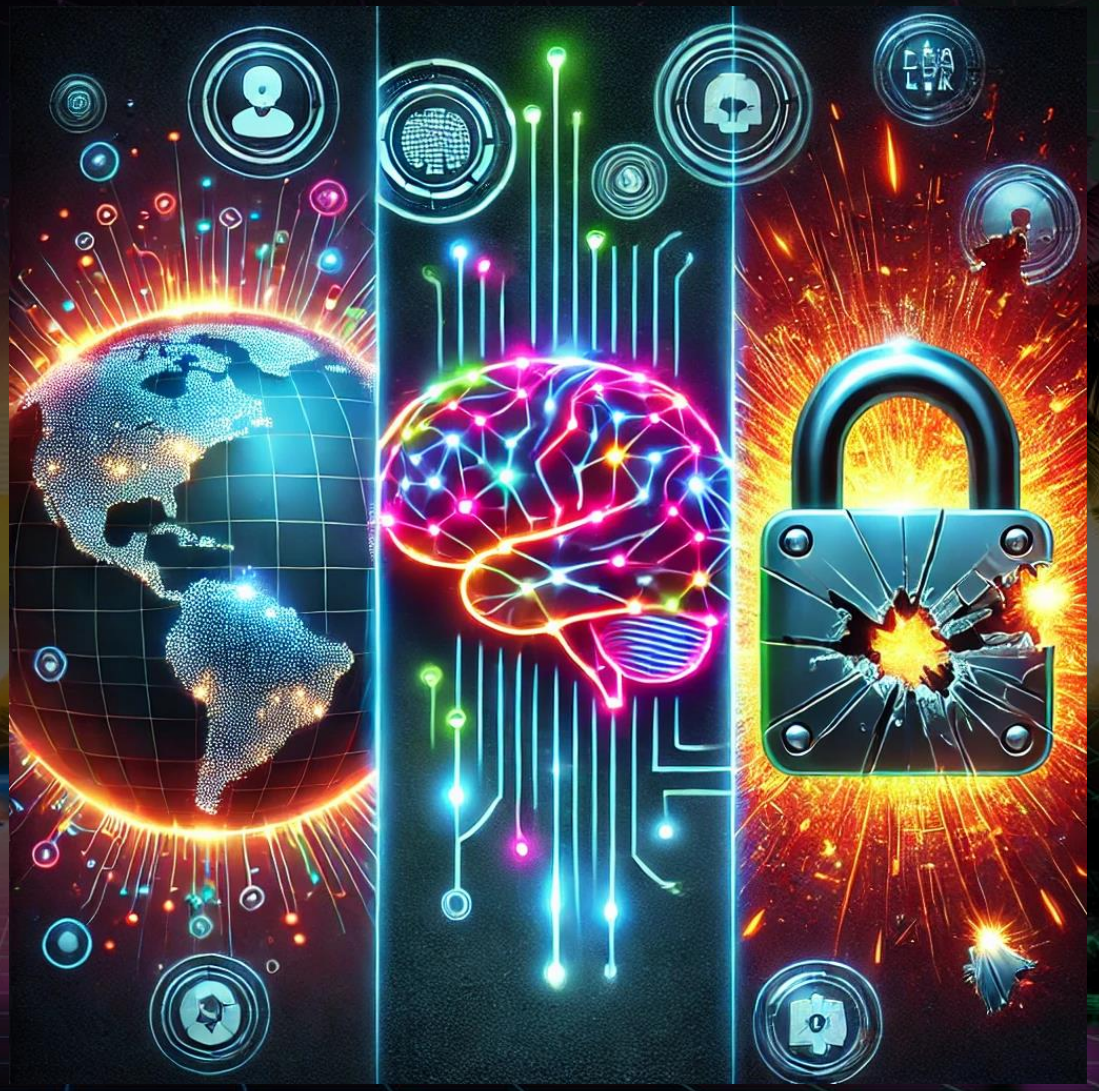
GenAI ANALYSIS:

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.

Trellix

GenAI powered Threat Intel



GenAI powered Threat Intel

I need you to generate a alluvian graph for threat actor mustang panda and its used tools? to generate the graph follow the instructions on the previous message

Used LangGraph

Based on the information provided by the STAR API about Mustang Panda, I'll create an alluvial graph showing the relationship between the threat actor, their tools, and the targeted sectors. Due to the large number of tools and sectors, I'll focus on the top 10 most notable tools and top 10 targeted sectors for better visualization.

Trellix

“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

Trellix

Money for Nothing...

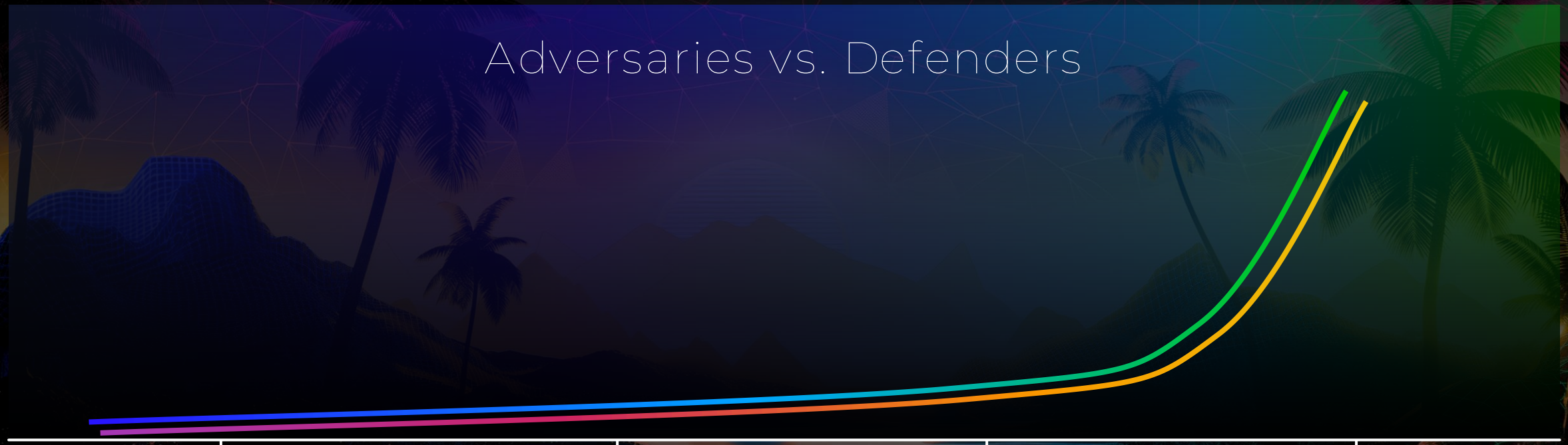
LockBit ransomware gang has over $110 million in unspent bitcoin

Trellix

But it does come at a price

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

AI Arms Race



Trellix

Defensive Urgencies

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

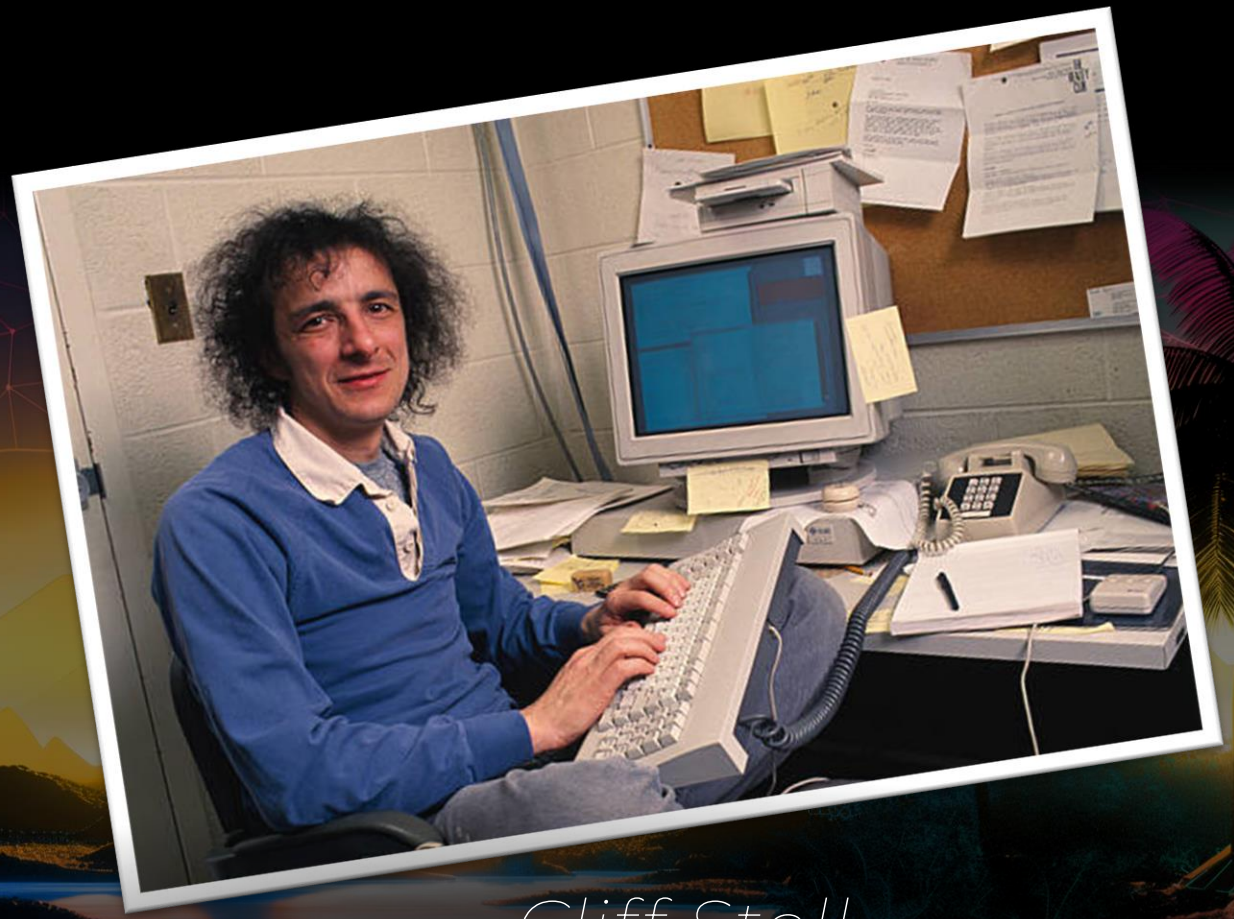
Zero Trust Mindset

"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

Trellix

Adaptive Sec Ops Pillars

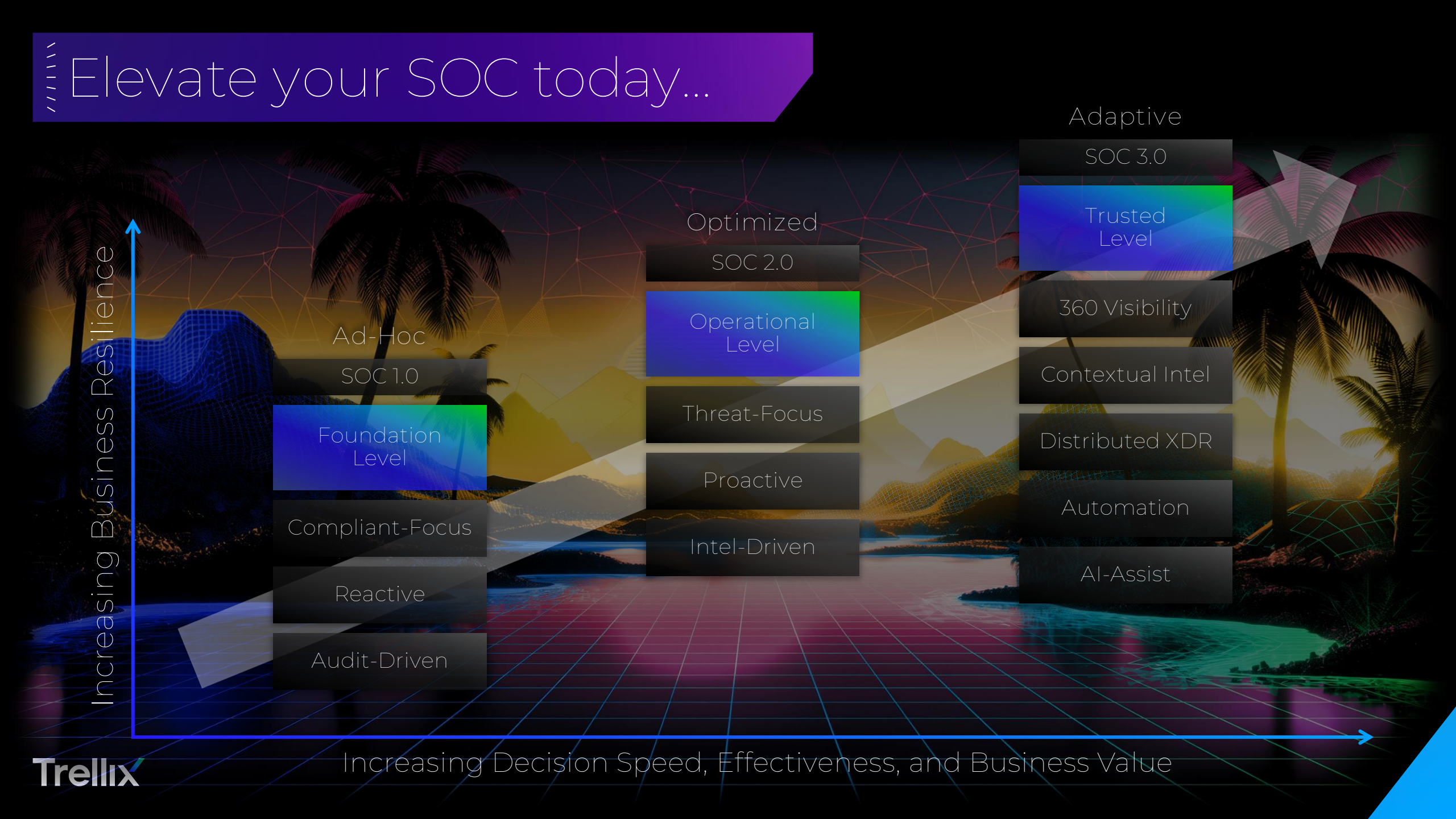
Incident Response

Threat Hunting

Exposure Management

Trellix

Elevate your SOC today...



Trellix

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)

Trellix XDR raises alert scores so analysts see them.

Alerts unseen for AI to investigate:
(Work remaining: 360 hours/day)

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

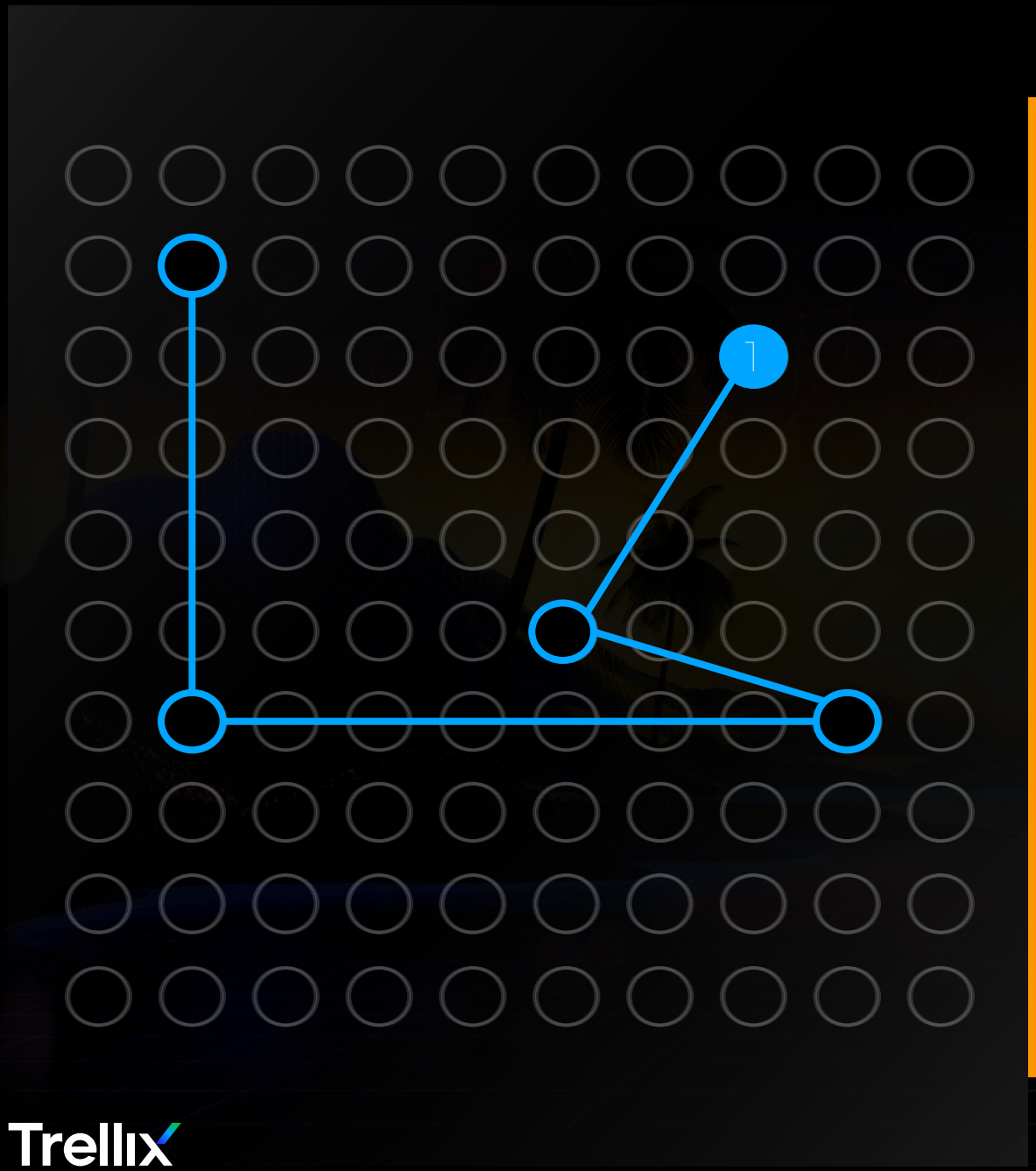
Find the Top 10 Things I need to investig

Hey John, This slide is being used by Martin

Trellix

Theory vs Reality...

Trellix



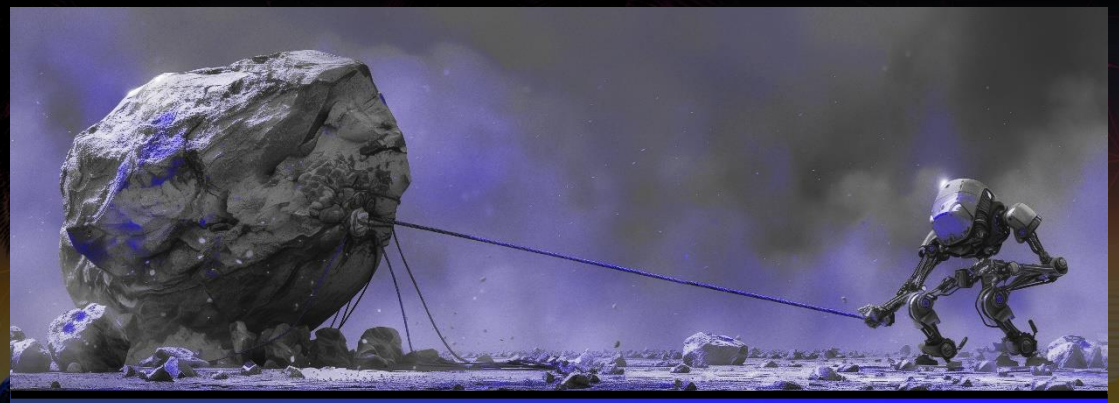
Generative AI XDR Solution:

1. Get some answers to specific questions (human time saved):
2. Is this user currently traveling? (3m)
3. Were there failed attempts before the password reset? (1m)
4. Does the user have an executive assistant? (1m)
5. What level of access does this user have? (3m)
6. What did they do after they reset the password? (5m)

Generative AI performs 13 minutes of work in under 45 seconds.

Trellix

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

Trellix

It's time to Come Together

Trellix