

06

Stop Looking Into Crystal Balls, Start Looking at Actual Signals

Speakers



Dor Goshier

Director of Product Management
Cyber Threat Intelligence

Most Predictions Fail

BITSIGHT
Luminate
EXCHANGE

BITSIGHT

©2026, BitSight Technologies, Inc. and its affiliates ("BitSight"). BITSIGHT® is a registered trademark of BitSight. All rights reserved.

Synnovis Incident



Primary Vector:

Stolen credentials;
lack of MFA



Impact:

1000+ operations
and appointments
cancelled

Type: Post | 06/24/2025, 12:00:00 AM |

Translate

6. CONFIDENTIALITY

a. **Non-Disclosure Obligations.** Recipient shall not disclose Confidential Information to any of its officers, directors, employees, contractors or agents or to any third party without the Discloser's written consent, except that (a) Recipient may disclose such information to its officers, directors, employees, contractors, and agents whose duties justify their need to know such Confidential Information, and who have been clearly informed of their obligation to maintain the confidential status of such Confidential Information, and in the case of contractors or agents, who have signed a written document acknowledging the obligation to maintain the confidential status of Confidential Information, and shall cause them to comply fully with these obligations, and (b) Recipient may disclose Confidential Information to the extent required by applicable federal, state or local law, regulation, court order, or other legal process, provided Recipient has given Discloser prior written notice of such required disclosure and, to the extent reasonably possible, has given Discloser an opportunity to contest such required disclosure at Discloser's expense.

b. **Protection of Confidential Information.** Recipient shall use the same care to prevent the unauthorized use or disclosure of Confidential Information as Recipient uses with respect to its own confidential information of a similar nature, which shall not in any case be less than the care a reasonable business person would use under similar circumstances. Without limiting the foregoing, Recipient shall take reasonable action by instruction, agreement or otherwise with respect to Recipient's employees or other persons permitted access to Confidential Information to cause them to comply fully with Recipient's obligations hereunder.

c. **Restricted Use Of Confidential Information.** Recipient may not use the Confidential Information directly or indirectly for any purpose other than the purpose for which it was originally disclosed, or for any purposes which could be deemed to be adverse to or competitive with Discloser or its business.

(d) **Return or Destruction of Confidential Information.** Upon written request recognition of the disclosure, Recipient shall either return or destroy all confidential information of the Discloser.

The provisions of this section (Confidentiality) shall survive any termination of this agreement.

7. CHOICE OF LAW

This agreement shall be construed and governed in accordance with the law of the Commonwealth of Massachusetts and any litigation shall be brought in the state or federal courts of the Commonwealth of Massachusetts.

8. INDEMNIFICATION

Stability shall indemnify, defend, and hold harmless Client, its affiliates, directors, officers, employees and agents from and against any and all such claims, demands, losses, damages, costs and expenses arising out of any third party claims arising from Stability's services including, without limitation, claims of

BEYOND THE HEADLINES

JUNE 29, 2025

FATAL ENCRYPTION: PATIENTS' DEATH LINKED TO CYBER ATTACK ON UK HEALTHCARE ORG

Image Text: 6. CONFIDENTIALITY a. Non-Disclosure Obligations. Recipient shall not disclose Confidential Information to any of its officers, directors, employees, contractors or agents or to any third-party without the Discloser's written consent, except that (a) Recipient may disclose such information to its of...

Why We're Blind

The Identity Problem:

80% of breaches involve compromised credentials

The Data Problem:

Over-reliance on tactical IOCs

The Sectoral Blind Spot:

Teams remain unaware they are being targeted until peers are already breached





Visionary

"Ai-driven", "flagship vendor" and "exemplar" for innovation, stating that "we are on the leading edge and setting the trend that the rest of the market should follow"

Roadmap discipline

clearly articulated roadmap, sustained execution with frequent incremental releases and quarterly strategic updates, and commitments to areas like AI-driven analysis and CTM

Broad integration and deployment flexibility

integrations across SIEM, SOAR, TIPs, identity tools, EDR/XDR, cloud, case management, and data-marketplace environments,



Predictions

Intelligence is concerned with the adversary's intent, capabilities, and opportunities.



Intent

What are potential attacker motives?
Financial, state sponsored, ideological
Who is being threatened?
Are you a potential victim or a deliberate target?



Capabilities

What are the tactics, techniques, and procedures available to the adversary?

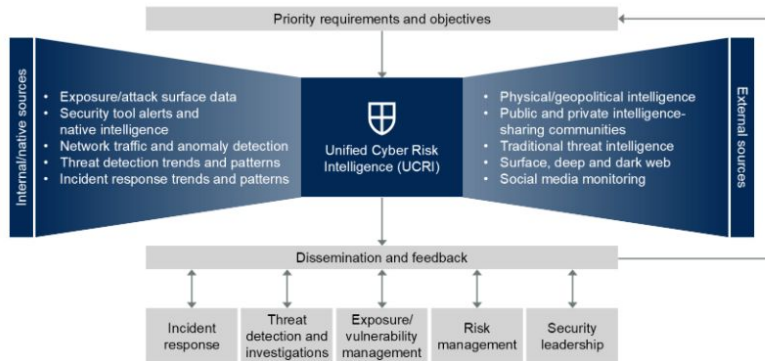


Opportunities

What element of your attack surface is being threatened?

The UCRI Framework: A New Mandate

UCRI Architectural Diagram

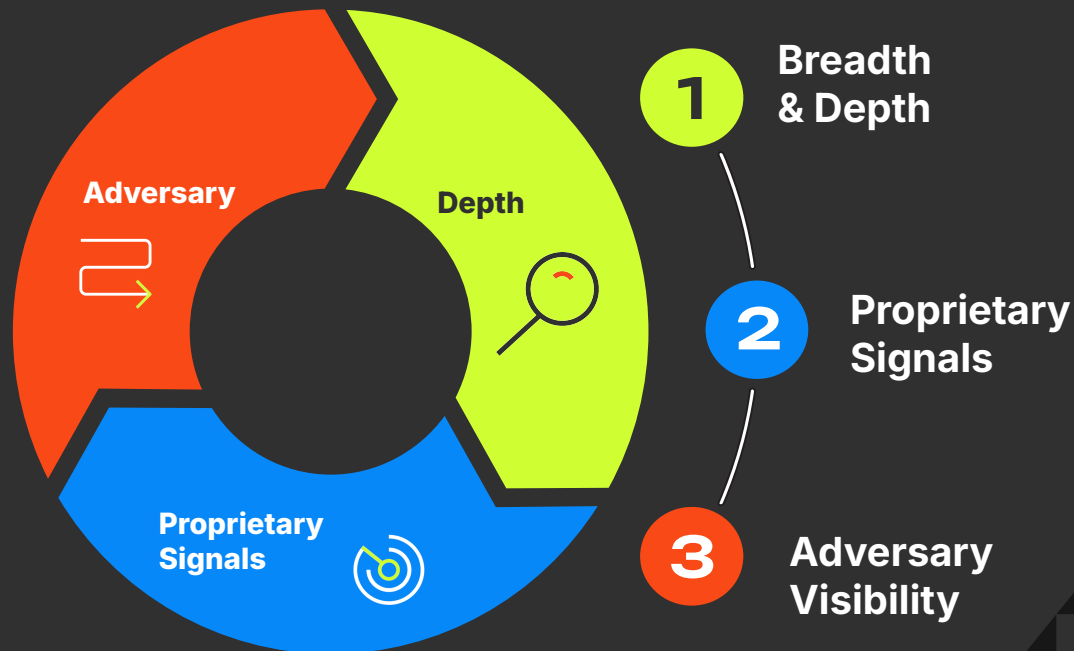


Source: Gartner
825638

Gartner

Data is only as good as its source

BITSIGHT
THREAT INTELLIGENCE



The Pillars of Preemption

01

Identity Intelligence

Detecting compromised credentials before weaponization

02

Adversary Intelligence

Real-time infrastructure and RW tracking

03

Brand intelligence

Identifying impersonation sites used for reconnaissance

04

Sectoral Intelligence

Early warning via peer-group monitoring.

05

Vulnerability intelligence

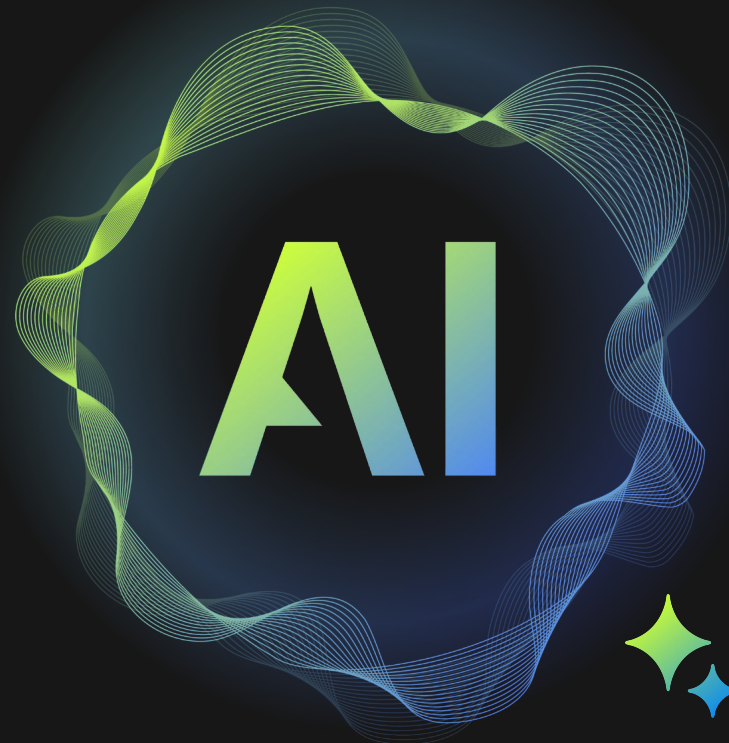
Deep/Dark Web insights into CVE exploitation probability.

Bitsight AI

Survival through synthesis

Predictive Alerting

Conversational Research and MCPs



Bridging the Gap CTI + Exposure Management

BITSIGHT
Luminate
EXCHANGE

BITSIGHT

©2026, BitSight Technologies, Inc. and its affiliates ("BitSight"). BITSIGHT® is a registered trademark of BitSight. All rights reserved.



Akira Attack

Reactive (Traditional)

Detection occurs at Day +10 during the encryption event - Too Late.

Proactive:

- Day -45: Exposure Management finds an unmapped VPN.
- Day -40: Vulnerability Intel flags VPN as active Akira target.
- Day -38: Identity Intel detects leaked VPN credentials.



Case Study: United Health & JLR



UnitedHealth / BlackCat: \$3B+ loss caused by stolen Citrix credentials lacking MFA.



Jaguar Land Rover: £1.9B loss; Jira logs harvested via stolen credentials months before systemic collapse

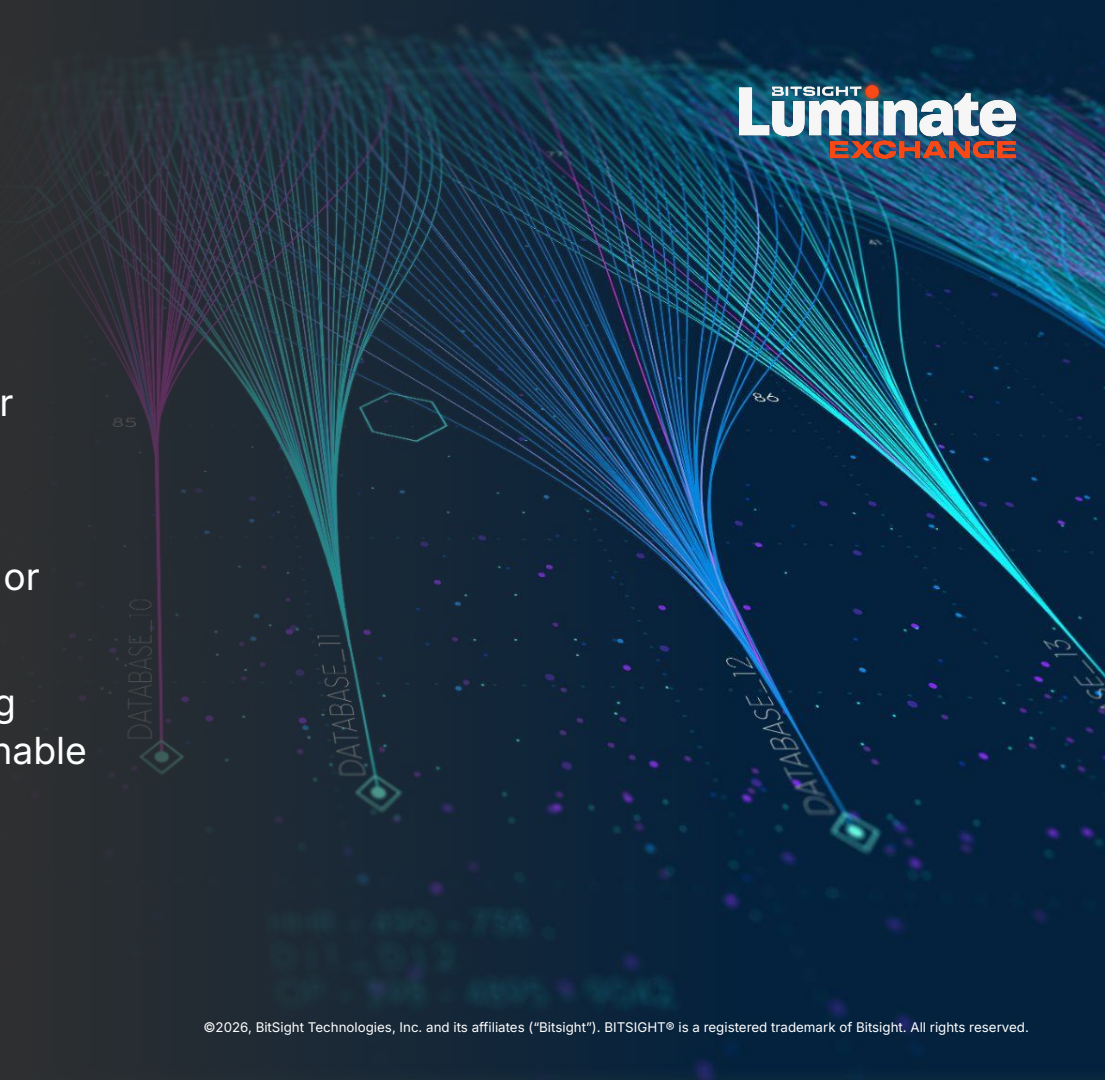


UCRI Value: Identity Intel flags keys weeks prior; Sectoral Intel identifies "reconnaissance surges" against peers.



Qilin Revisited

- **Third-Party CTI Monitoring:** "Verified Victim" alerts identify supplier targets before disruption.
- **Identity Intelligence:** Proactive detection of credentials on RDP shops or Russian markets.
- **Sectoral Intelligence:** Monitoring shifts toward supply chain targets to enable "Air Gap" preparations.



SUMMARY

From collecting IOCs to validating defense performance



- **Modular Defense:** Integrating Identity, Sectoral, and Exposure Intelligence to close the visibility gap.
- **The Outcome:** Disrupting the kill chain weeks before encryption.
- **Business Value:** Moving from "Patch Everything" to "Patch What Matters".

BITSIGHT

BITSIGHT
Luminate
EXCHANGE

 **Thank you**

For more information, please contact:

Dor Goshier

Director of Product Management, Cyber Threat Intelligence

BITSIGHT

©2026 BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.