

“

# Next-Generation Threat Hunting

How AI Transforms Detection and Response



Mark Hassoun  
Technical Director



# AI-Powered Cyber Attacks: the new normal

CYBERSECURITY · APRIL 2026

## AI-powered attacks: the new normal

Key numbers from IBM X-Force, CrowdStrike, Gartner & Pindrop

**340%**

Rise in AI-assisted intrusions vs. 2024  
CrowdStrike 2026

**87%**

Of organizations hit by an AI attack in 2025  
SoSafe / IRONSCALES

**\$5.72M**

Avg. cost of an AI-powered breach in 2025  
IBM Cost of Breach

**\$10.5T**

Projected global cybercrime losses in 2025  
SentinelOne / Gartner

### SECTORS & REGIONS MOST TARGETED

#### Top sectors

IBM X-Force 2026 · SQ Magazine

Manufacturing **27.7%**  
of all incidents

Finance & insurance **18.2%**  
of all incidents

Energy & utilities **11.1%**  
of all incidents

Healthcare (AI attacks) **+76%**  
YoY rise

#### Top regions

IBM X-Force 2026 · SQ Magazine

North America (up from 24% in 2024) **29%**  
of all cases

Asia-Pacific AI-enabled attacks **+56%**  
YoY rise

Europe (Germany & UK top targets) **28%**  
of AI breaches

Middle East AI espionage campaigns **+31%**  
YoY rise

### WHAT'S DRIVING THE SURGE

Phishing emails now AI-generated

**82.6%**  
IRONSCALES 2025

Malware with AI-driven polymorphism

**76%**  
IRONSCALES 2025

Ransomware groups active (49% surge YoY)

**135+ groups**  
IBM X-Force 2026

Attacks via exploited apps — YoY increase

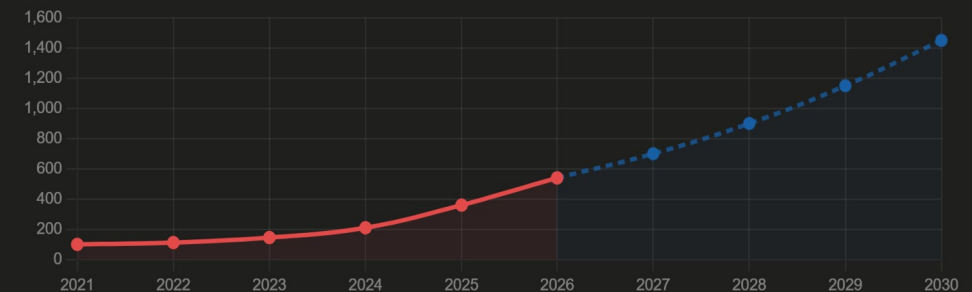
**+44%**  
IBM X-Force 2026

Supply chain compromises vs. 2020

**4× higher**  
IBM X-Force 2026

### ATTACK GROWTH FORECAST — INDEXED (2021-2030)

Actual Projected



Indexed projections based on CrowdStrike, Gartner & AllAboutAI trend analysis · 2021 = 100 baseline



## CYBERSECURITY LANDSCAPE SHIFT

- AI-powered attacks
- More sophisticated and targeted
- Attackers are faster
- Attackers are always-on





## SO, AI INTRODUCES NEW SECURITY CHALLENGES

- Using AI to enhance cybersecurity
- Defending against AI-powered attacks
- Protecting AI systems themselves

# The Limitations of Today's Cyber Security Tools



Data Explosion



Legacy SIEM Architecture



Scalability Challenges



Analysts Skills Gap



Alarms Fatigue



No AI/ML Capabilities



No Single Reliable  
Source of Intel



# SUCCESS IN THIS NEW AI-DRIVEN ERA DEPENDS ON THREE CORE CAPABILITIES

1

## UNIFIED DATALAKE

Bringing all  
information together

2

## AI DECISION SYSTEMS

Automating analysis  
and response

3

## CONTEXTUAL INTELLIGENCE

Understanding  
threats and data  
relationships



# CLOUD-NATIVE DATA LAKE



**Efficiency:** Ingest and search separated → **Decoupled Storage from Compute.**



**Performance:** **always-hot** compute & storage (no rehydration)



**Scalability:** Elastic scaling to **millions of cores** on-demand.



**Cloud Native:** Deep **AWS optimization** with patented processes.

## 300X FASTER DETECTION AND INVESTIGATION

Analysts pivot across years of data and intelligence in seconds.

## 96% REDUCED TIME FOR THREAT INVESTIGATIONS

Context-driven prioritization reduces false positives and alert fatigue.

## 50% ANALYST TIME SAVED WITH OPERATIONALIZED INTEL

Threat intel informs every stage of the SOC workflow, not just reports.

## 60% REDUCED SIEM BILL AND OPERATIONAL COST

Eliminate SIEM tax and manual effort while scaling data retention.



# Threat Hunting made easier with Generative AI



What are the top threats to my organization?



ASK ANOMALI AGENTIC AI

The top threats to your organization over the last 30 days include: Actors: Chaos, FSB, Federal Security Service, Hamas, Laravel, Opsec, Payouts, Scam\_Guard, Silent Crow, World Leaks. Attack Patterns: Application Layer Protocol, Command and Scripting Interpreter, Deobfuscate/Decode Files or Information, Exploitation for Client Execution, Exploitation for Privilege Escalation, Impair Defenses: Disable or Modify Tools, Ingress Tool Transfer, Masquerading, System Information Discovery, Valid Accounts. |



Tell me about IP 118.248.255.174



ASK ANOMALI AGENTIC AI

The IP address 118.248.255.174 is identified as a malicious IP (mal\_ip), an APT IP (apt\_ip), and a scanning IP (scan\_ip) with high confidence levels ranging from 98 to 100. It has been tagged with various sources such as Mandiant, Anomali Adversary Intelligence, and cinscore:ci-badguys OSINT. It is located in China and is part of the China Unicom Shandong province network. The IP is associated with the threat actor APT28, known for state-sponsored activities and information theft. Tags related to APT28 include Fancy Bear and Iron Twilight.



# Global & Vertical Threat Landscape



## Threat Landscape: Global

360° View of the Threat Landscape providing visibility into global attack trends, vertical-specific risks, and threats directly impacting your organization.

Global Vertical Last 30 days

### Global Curated News Articles

02 Oct 2025

#### Critical Vulnerability in Popular VPN Service Affects Millions

Security researchers discovered a critical vulnerability in a widely used VPN service that...

02 Oct 2025

#### New Ransomware Group Targets Multiple Industries

A newly identified ransomware group named 'BlackShadow' has been targeting organizations...

01 Oct 2025

#### Major Tech Companies Form Alliance to Combat Supply Chain Attacks

Leading technology companies announced a new collaborative initiative to develop shared security...

01 Oct 2025

#### Zero-Day Exploit Found in Widely Used IoT Devices

Security researchers have identified a zero-day vulnerability affecting millions of IoT devices that...

### Targeted Entities

#### Most Targeted Entities

#### Memorial Health System Healthcare

↑ +27% Last 30 days

Targeted for patient data and ransomware opportunities.  
Attack vectors: Phishing, Unpatched VPNs

#### First National Bank Finance

↑ +18% Last 30 days

Targeted for financial fraud and customer data theft.  
Attack vectors: Web App Exploits, Social Engineering

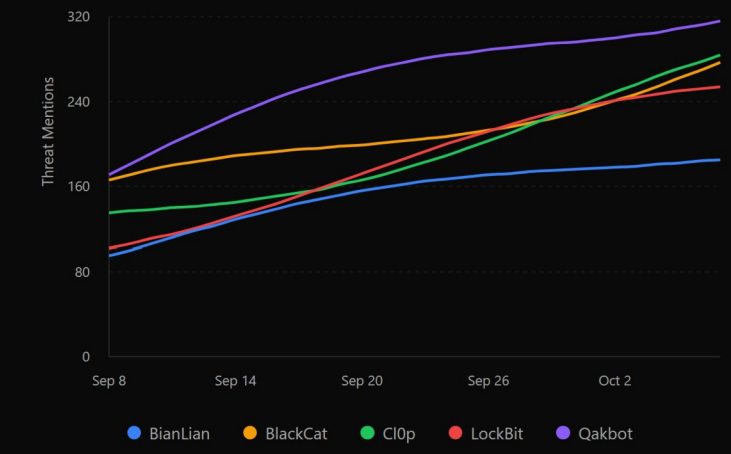
#### CloudServe Technologies Infrastructure

↑ +32% Last 30 days

Targeted for data breaches and service outages.  
Attack vectors: Denial of Service, Malware

### Trending Malware Threats

#### Threat Landscape



#### Top Threats

<b>Qakbot</b> Malware Distribution	342	↑ 22.1%
<b>BlackCat</b> Ransomware	287	↓ 7.4%
<b>Cl0p</b> Ransomware	265	↑ 39.5%
<b>LockBit</b> Ransomware	243	↓ 4.7%
<b>BianLian</b> Ransomware	198	↑ 41.4%

### Trending Vulnerabilities

CVE-2023-29298

Great Developers Ce...

+ Ask anything, perform tasks and get your job done Copilot

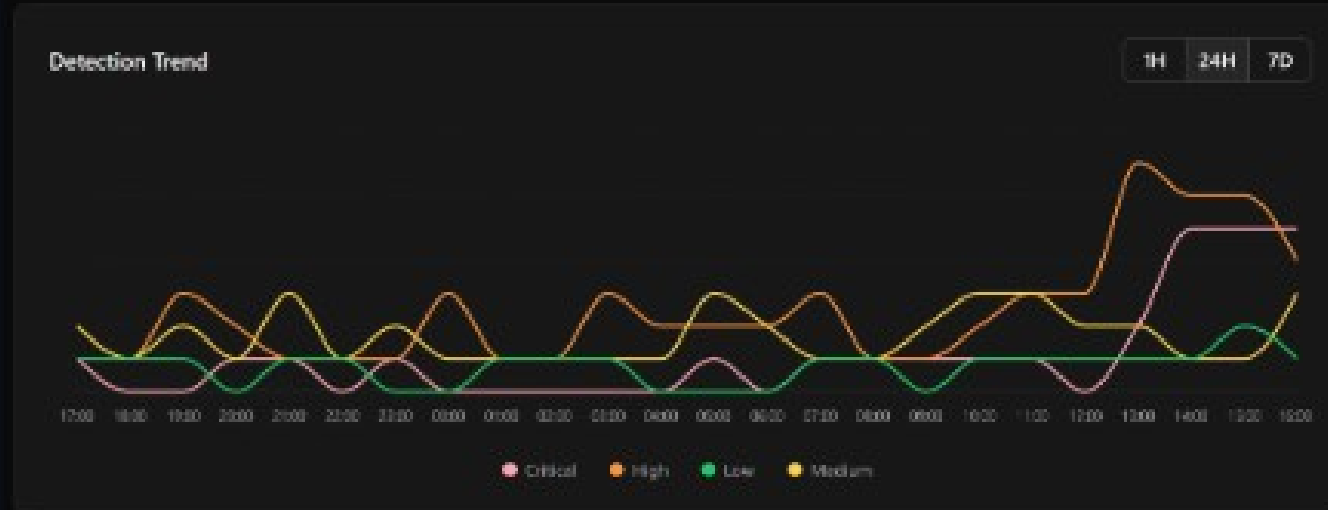


# Security Coverage Mapped Detections

## Detections

Individual detection events fired by active rules.

Live



Detection Rule Matches | IOC Matches | DGA Matches

Search rules & entities... Severity: Critical 43 | DCSP Category | Entry Type | Detection Rule | Reset | Time Range: Last 24h | Hide False Positives

Rule	Category	Severity	Count	Trend	Last Seen	
> Excessive Failed Logins	Authentication	High	50		15 Apr 2026 16:02:04	...
> Impossible Travel Detection	Authentication	Critical	8		15 Apr 2026 15:32:32	...
> Lateral Movement via SMB	Network Activity	Critical	12		15 Apr 2026 16:06:13	...

+ Ask anything, perform tasks and get your job done Copilot



# Zero Day Detections with ML Analytics

### User Details

**Sarah Chen** 36 Current Risk Score  
Medium

User Active Directory

Overview Risk Score Detections Associated Entities History

**36** Risk Score   **3** Detections   **1** Alerts   **0** Incidents

#### Details

Full Name	Sarah Chen	Email	sarah.chen@company.com
Title	Senior Software Engineer	Department	Engineering
Manager	Michael Torres	Employee ID	EMP-1001
Status	Active	Last Login	25 Feb 2026 09:15
Source	Active Directory		

### User Details

**Sarah Chen** 36 Current Risk Score  
Medium

User Active Directory

Overview **Risk Score** Detections Associated Entities History

#### Copilot Risk Score Summary

Sarah Chen has a risk score of 36 (Medium), primarily driven by 3 detections including "Unusual login location". Membership in Engineering, Backend, High Profile Users applies a combined multiplier of  $\times 2.8$  to the base score. Current risk levels are within acceptable thresholds.

Generated by Copilot

#### Risk Score Over Time

Peer group: High Profile Users   30 days

### User Details

**Sarah Chen** 36 Current Risk Score  
Medium

User Active Directory

Overview Risk Score Detections Associated Entities **History**

- 24 Feb, 00:00 🔒 Detection: Unusual login location  
Base risk contribution: 4
- 23 Feb, 00:00 🔒 Detection: Sensitive file access  
Base risk contribution: 5
- 22 Feb, 00:00 🔒 Detection: After-hours VPN connection  
Base risk contribution: 3
- 24 Feb, 00:00 📈 Risk score updated to 36  
Calculated from 3 detections with group multiplier  $\times 2.8$



# Agentic AI SOC

## My Agents

Monitor and manage your active AI agents.

10 / 5 agents enabled



Search agents...

Status

Trust Level

Agent Name	Role	Status	Decision Quality	Hours Saved / Week	Other Metrics	Schedule
Alice	CTI Specialist	Idle	51%	5h 15m	PIRs managed: 6, Feeds monitored: 8	Weekly - Monday 06:00 UTC
Marcus	SDC IS Analyst	Running	81%	3h 30m	Rules tuned: 9, False positives suppressed: 141/wk	Continuous
Riya	IR Specialist	Idle	—	0h	—	Event-triggered
Leo	Geopolitical Risk	Idle	—	0h	—	Weekly - Wednesday 09:00 UTC
Nadia	Financial Risk	Idle	91%	1h 15m	Threat actions tracked: 7, Indicators monitored: 94	—
Joshua	Threat Hunter	Idle	—	0h	—	—
Victor	Vulnerability Management	Idle	—	0h	—	—
Grace	GRC	Idle	—	0h	—	—

+ Ask anything, perform tasks and get your job done Copilot



# LLM-to-LLM MCP Integrations

<b>THREAT ACTORS</b> 54 Targeting UAE from Iran	<b>IOCS COLLECTED</b> 209 Iran tagged, Apr 10-15	<b>THREAT BULLETINS</b> 334 Iran-related, April 2026	<b>ACTIVE CAMPAIGNS</b> 19 Iran → UAE linked
---	--	--	--

### Key Iranian threat actors targeting UAE

- APT34 / Helix Kitten (APT) Energy, Gov
- APT42 (APT) Education, Gov
- Handala (Hacktivist) Energy, Finance
- MuddyWater / Static Kitten (APT) Gov, Telecom
- UNC1860 (APT) Energy, Telecom
- Stormous (Ransomware) Finance, Gov
- APT33 / Nemesis Kitten (APT) Aerospace, Energy
- Imperial Kitten (APT) Defense, Energy

Legend: State-sponsored APT (Red), Hacktivist (Orange), Ransomware (Blue)

### IOC breakdown (Apr 10-15)

21 Malicious hashes	24 Malicious files	5 Malicious domains
---------------------	--------------------	---------------------

### Severity distribution

Very High	21
High	25
Medium	4

### IOC types (itype)

mal_md5	21
mal_file_name	21
mal_domain	5
mal_ssdeep	3

### Targeted Industries

Energy / Oil & Gas	High
Government	High
Financial services	Medium
Telecom	Medium

### Key MITRE ATT&CK techniques observed

T1566.002	Spear-phishing link	Critical
T1219	Remote access software	Critical
T1565	Data manipulation	High
T1486	Data encrypted for impact	High

## MCP servers

Discover and manage MCP servers that you're working on.

Configure

threatstream

threatstream running

Command

npx

Arguments

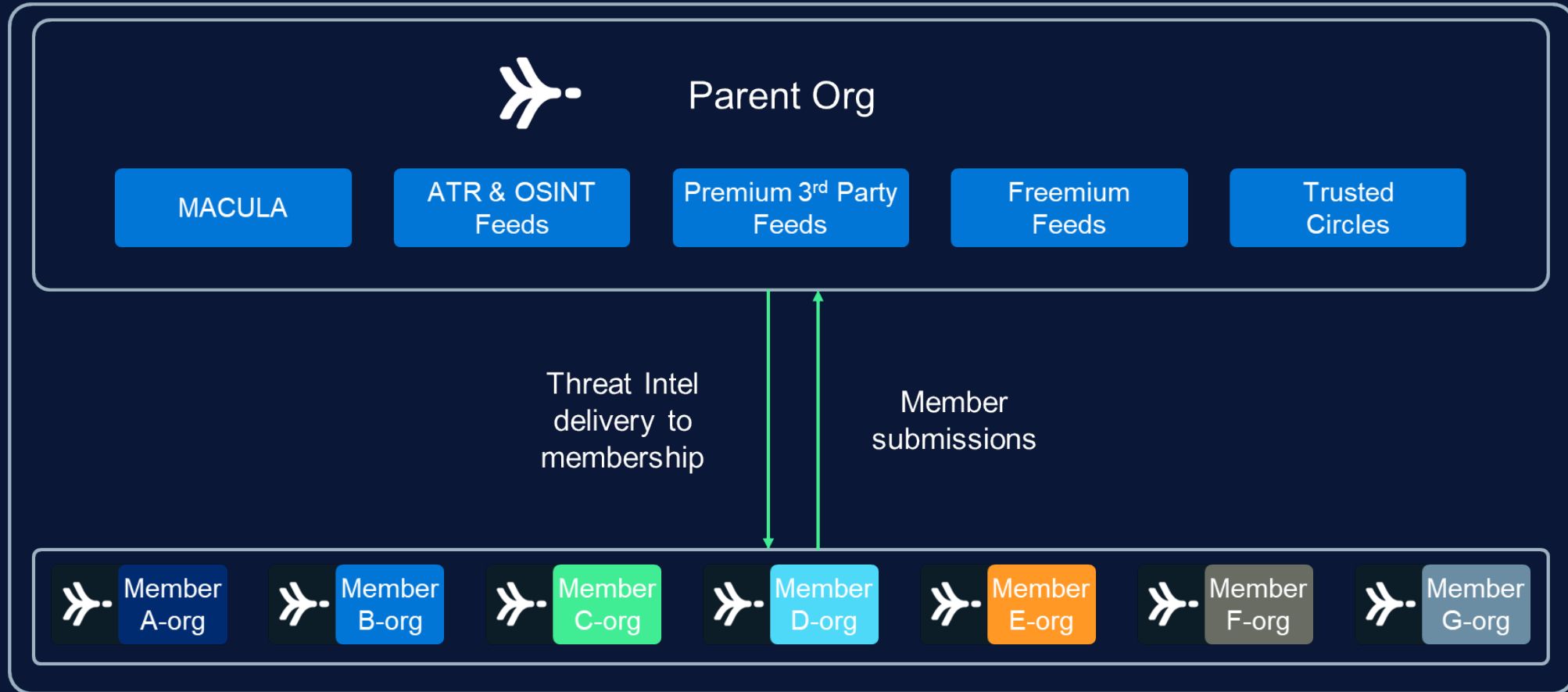
mcp-remote https://optic.threatstream.com

View Logs

> Advanced options



# ISACs & ISAOs Intel Sharing



ANOMALI