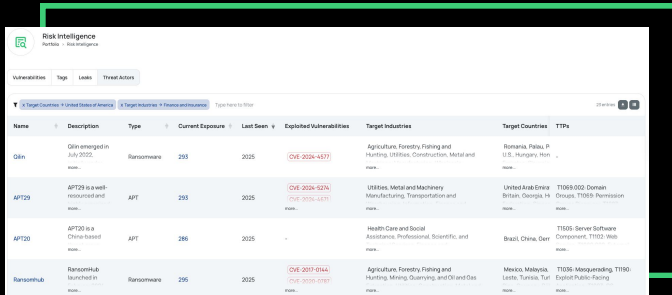


Turn Threat Actor Intelligence into Third-Party Risk Action



Name	Description	Type	Current Exposure	Last Seen	Exploited Vulnerabilities	Target Industries	Target Countries	TTPs
Glin	Glin emerged in July 2022.	Ransomware	255	2025	CVE-2024-4371	Agriculture, Forestry, Fishing and Hunting, Utilities, Construction, Metal and more	Romania, Italy, P, U.S., Hungary, Hon	
APT29	APT29 is a well-resourced and	APT	255	2025	CVE-2024-5274 CVE-2024-4371	Utilities, Metal and Machinery, Manufacturing, Transportation and more	United Arab Emira, Britain, Georgia, Is	T109: 002, Domain, C2: 003, T109: 003, T109: 003
APT20	APT20 is a China-based	APT	286	2025		Health Care and Social Assistance, Professional, Scientific, and more	Brazil, China, Ger	T109: 002, Domain, Component, T109: 003
RansomHub	RansomHub	Ransomware	255	2025	CVE-2021-0144 CVE-2020-2187	Agriculture, Forestry, Fishing and Hunting, Mining, Quarrying, and Construction, and more	Mexico, Malaysia, Latvia, Turkey, Tur	T109: 002, Domain, T109: 003, T109: 003

THREAT ACTOR INTELLIGENCE

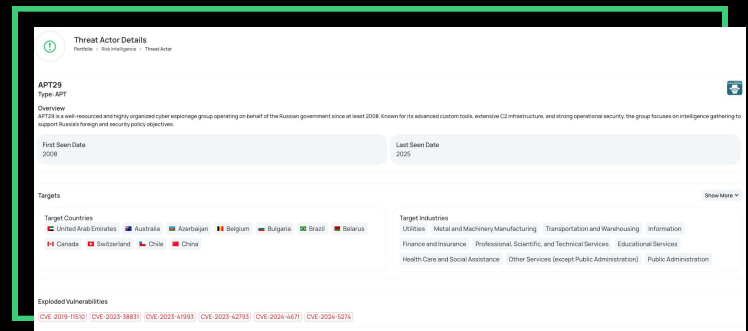
Quickly identify which vendors align with known adversary profiles

- Uncover which industries and regions specific threat actors are actively targeting
- Instantly identify the adversaries most relevant to your third parties
- Understand how your extended supply chain fits into current attack trends

DEEP ADVERSARY PROFILES

Access detailed threat actor playbooks to anticipate behavior and sharpen response

- Access detailed profiles outlining each actor's TTPs, exploited vulnerabilities, and targeting behavior
- Map adversary behavior to the MITRE ATT&CK Framework for standardized intelligence
- Equip your team with insights to anticipate and counter known adversary strategies

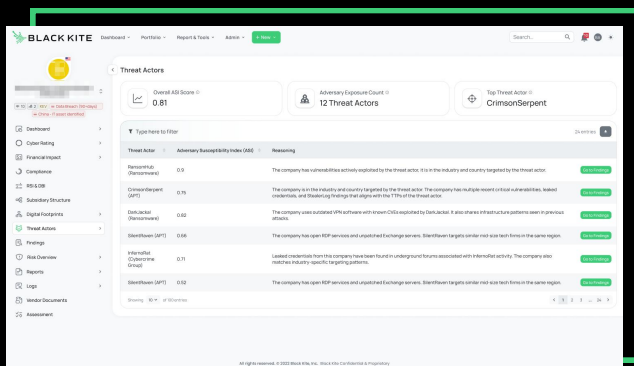


Threat Actor Details	
APT29 Type: APT	
Overview APT29 is a well-resourced and highly organized cyber espionage group operating on behalf of the Russian government since at least 2008. Known for its advanced custom tools, extensive C2 infrastructure, and strong operational security, the group focuses on intelligence gathering to support Russian foreign and security policy objectives.	
First Seen Date	Last Seen Date
2008	2025
Targets	
Target Countries United Arab Emirates, Australia, Azerbaijan, Belgium, Bulgaria, Brazil, Belarus, Canada, Switzerland, China, China	Target Industries Utilities, Metal and Machinery Manufacturing, Transportation and Warehousing, Information, Finance and Insurance, Professional, Scientific, and Technical Services, Educational Services, Health Care and Social Assistance, Other Services (except Public Administration), Public Administration
Exploited Vulnerabilities CVE-2019-11930 , CVE-2023-38831 , CVE-2023-41991 , CVE-2023-42765 , CVE-2024-4371 , CVE-2024-5274	

VENDOR-LEVEL SUSCEPTIBILITY MAPPING

Visualize and act on the specific ways threat actors could exploit your vendor ecosystem

- See which vendors are susceptible to which adversaries, across your portfolio
- Access mapped findings with technical evidence behind each ASI score
- Prioritize and guide remediation efforts with threat-specific reasoning



Threat Actor	Adversary Susceptibility Index (ASI)	Reasoning
RansomHub (Ransomware)	0.9	The company has vulnerable data activity exploited by the threat actor. It is in the industry and country targeted by the threat actor.
BlackKite (APT)	0.75	The company is in a high industry and country targeted by the threat actor. The company has multiple recent critical vulnerabilities, leaked credentials, and bleeding through that align with the threat actor's threat actor.
BlackKite (Ransomware)	0.65	The company uses outdated VPN software with known CVEs exploited by the threat actor. It also shares infrastructure patterns seen in previous attacks.
BlackKite (APT)	0.65	The company has open RDP services and unpatched exchange servers. BlackKite targets similar mail servers from the same region.
BlackKite (APT)	0.71	Leaked credentials from the company have been found in underground forums associated with information activity. The company also machine industry specific targeting patterns.
BlackKite (APT)	0.52	The company has open RDP services and unpatched exchange servers. BlackKite targets similar mail servers from the same region.