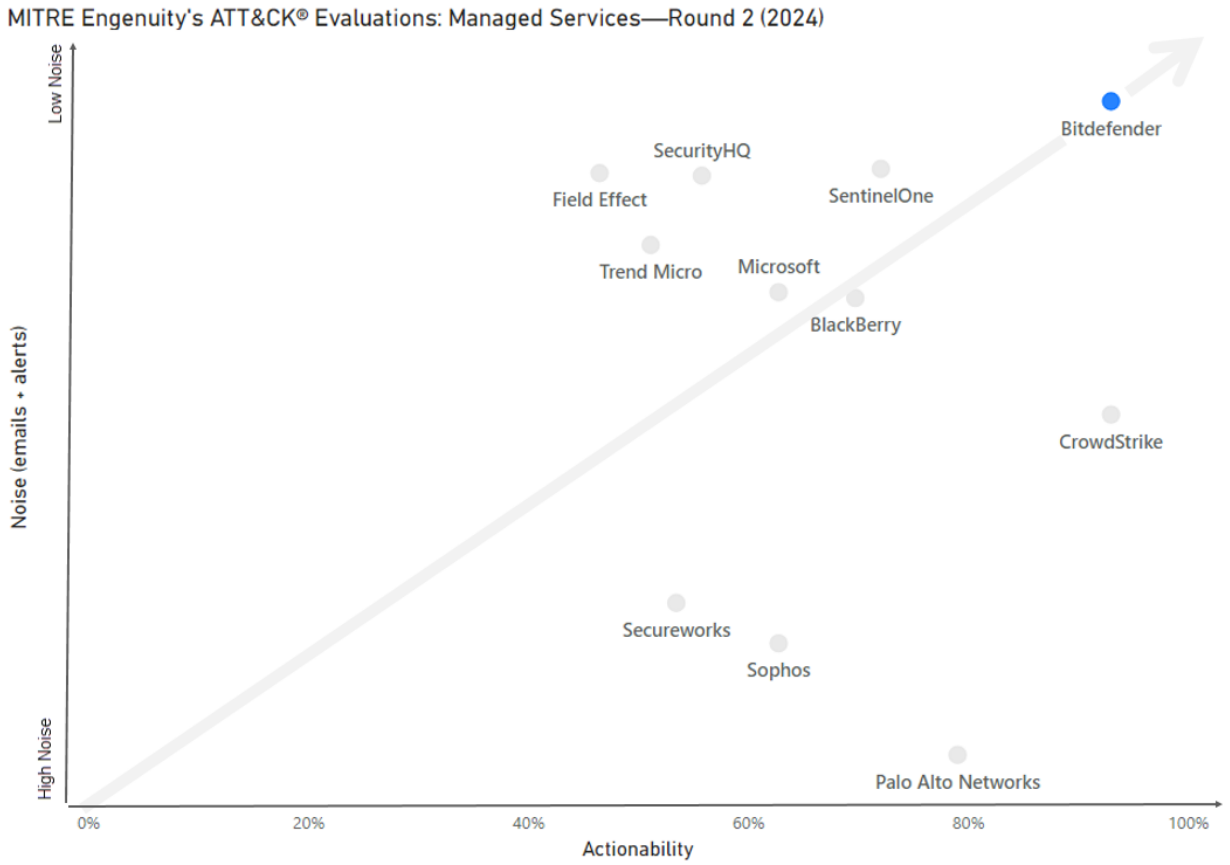
Bitdefender

DATASHEET

Bitdefender's Top Performance in the MITRE Engenuity ATT&CK Evaluations for Managed Services

MITRE Engenuity is a tech foundation aimed at working with the cybersecurity private sector to foster good competition and collaboration with the goal of improving the cybersecurity landscape. The 2024 ATT&CK Evaluations for security service providers tested participating cybersecurity vendors in a 'closed book' version of adversary emulation using tactics, techniques and procedures (TTPs) of BlackCat/ALPHV, a prolific ransomware-as-a-services (RaaS) group, and menuPass (aka APT10), an advanced threat actor focused on espionage targeting an array of industries including healthcare, manufacturing and government.

In the recently published results, Bitdefender came away as one of the top performers in the evaluation with 100% visibility of the attacks, one of the lowest mean times to detect (MTTD) while reducing the most noise and providing clear and actionable alerts.



Bitdefender

DATASHEET

While many participants successfully detected and reported on the threat and adversary tactics, very few were able to do so in a manner that showcased the value and benefit of their managed service offerings. Let's look at some key datapoints from the results:

		Bitdefender	BlackBerry	CrowdStrike	Field Effect	Microsoft	Palo Alto Networks	Secureworks	SecurityHQ	SentinelOne	Sophos	Trend Micro	Mean	Median
Coverage Quality	Visibility (data collected)	43	42	43	41	43	43	43	43	43	43	43	43	43
	Reported (not actionable)	41	35	42	25	37	38	25	33	38	36	36	35	36
	Reported (actionable)	40	30	40	20	27	34	23	24	31	27	22	29	27
	Were any Red Team activities missing from incident reports?	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	N/A	N/A
Speed	MTTD (minutes)	24	48	4	11	24	24	33	93	47	72	65	41	33
Noise	Emails + Alerts	82	394	579	196	385	1119	878	200	189	942	310	479	385
	Total Emails	54	307	326	98	162	37	51	125	32	24	138	123	98
	Total Alerts in Console	28	87	253	98	223	1082	827	75	157	918	172	356	172

Mean Time to Detect (MTTD) and Alerts

A key benefit of any Managed Service offering is to reduce the MTTD - mitigating threats as early as possible - while also reducing the amount of noise and alerts a customer receives. While some vendors had incredibly low MTTDs, it was often paired with an abundance of alerts which in a real-world scenario would translate to alert fatigue for their customers.

Bitdefender was able to detect the malicious activity within 24 minutes of the event occurring while heavily reducing the number of alerts sent to the customer. Customers receiving an alert notification from us will know that we conduct deep investigations and that the information we pass along is accurate and credible.

Actionability

While filtering noise and benign events is important, what you alert or report on must also include context, details, and "actionability" to ensure proper action is taken to address or remediate the threat. Again, we can see that Bitdefender had the highest percentage (93%) of actionable reporting in the evaluations showcasing our ability to help our customers respond to threats and remediate malicious activity.

The Bottom Line

Customers turn to Managed Services, and especially Managed Detection and Response (MDRs), to help supplement their security team, alleviating many of the responsibilities they do not have the time or security expertise for. When reviewing evaluations like MITRE Engenuity, it's important to focus on the datapoints that can help your team and organization be more secure. If ensuring timely and accurate detections with actionable insight is important to you, reach out to us today.

08082024 Bitdefender-BSG-MITREEVAL-Datasheet-creat7936-en_EN