In this testing, MITRE took on the persona of APT29, a threat group that has been attributed to the Russian government and has operated since at least 2008.

Other aliases: Cozy Bear, The Dukes, YTTRIUM
They attacked participant environments using two scenarios. These scenarios were publicly reported to match the tradecraft and operational flows followed by the group APT29.
How this evaluation differs

Adversary-centric vs. Malware-centric

MITRE Evaluation tests how solutions detect an adversary performing a targeted attack. It does not test a product’s ability to block/prevent malware.
Participants included:

- FireEye
- Bitdefender
- Cybereason
- Cycraft
- Elastic
- F-Secure
- HanSight
- Malwarebytes
- ReaQta
- Secureworks
All detections (not prevention) were recorded across every step of the attack.

Results

- Detected Automatically
- Detection enriched using Trend Micro’s Managed XDR team
- Not Detected
However the challenge is, no clear scoring is given.

"We show the detections we observed without providing a ‘winner.’ There are no scores, rankings, or ratings. Instead, we show how each vendor approaches threat defense within the context of ATT&CK."

— MITRE
Then how well did Trend Micro do?
#1 in Initial Overall Detection

Leader
Detection Rate With Initial Configuration
(Out of a 78% average)

91%  (Trend Micro)
90%  (SentinelOne)
89.5% (Cortex)

Wait... What about...

86%  (CrowdStrike)
76%  (VMware Carbon Black)
84%  (Symantec)

© 2020 Trend Micro Inc.
Detections without configuration changes
Detections after configuration changes
Key Highlights – Fewest Missed Detections

- Lowest number of missed detections among all vendors – initial configuration
Key Highlights – Strong Technique Detections

- Detected very well on individual attack techniques, which are higher confidence detections.
Key Highlights – Actionable Alerts

- Managed alert volumes to avoid alert fatigue.
- Lower level of alerts combined with high detection rate means we reduced the noise of all detections into a minimal amount of meaningful/actionable alerts.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Detection Rate</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrendMicro</td>
<td>91.04%</td>
<td>24</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>90.30%</td>
<td>51</td>
</tr>
<tr>
<td>Microsoft</td>
<td>89.55%</td>
<td>33</td>
</tr>
<tr>
<td>PaloAltoNetworks</td>
<td>89.55%</td>
<td>50</td>
</tr>
<tr>
<td>F-Secure</td>
<td>88.06%</td>
<td>38</td>
</tr>
<tr>
<td>FireEye</td>
<td>88.06%</td>
<td>54</td>
</tr>
<tr>
<td>Elastic</td>
<td>87.31%</td>
<td>46</td>
</tr>
<tr>
<td>CrowdStrike</td>
<td>85.82%</td>
<td>22</td>
</tr>
<tr>
<td>Symantec</td>
<td>84.33%</td>
<td>21</td>
</tr>
<tr>
<td>Secureworks</td>
<td>82.09%</td>
<td>34</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycraft</td>
<td>80.60%</td>
<td>90</td>
</tr>
</tbody>
</table>
Key Highlights – Strong Telemetry

- Telemetry = Visibility. We give security analysts access to the type and depth of visibility they need when looking into detailed attacker activity.
Key Highlights – MDR Enriched Detections

• Our detection coverage results would have remained strong without MDR service, though the service was able to add more valuable context.
References

• MITRE Evaluation results (APT29):

• Blog posts:
  – https://blog.trendmicro.com/top-ten-mitre/

• Forrester assessment:
  – https://github.com/joshzelonis/EnterpriseAPT29Eval
Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**