PICUS TREND MICRO | XDR

INTEGRATION BRIEF

THE PICUS COMPLETE SECURITY VALIDATION PLATFORM AND TREND MICRO VISION ONE XDR INTEGRATION

INTEGRATION OVERVIEW

The Picus Complete Security Validation Platform integrates with **Trend Micro Vision One XDR** to enable joint users to automatically simulate real-world threats and ensure that detection policies are continuously tuned to identify and alert on them.

Overall benefits of the joint integration are security teams being able to achieve a more proactive approach to threat detection, alleviate manual detection engineering processes, and reduce false positive alerts.

Security Validation

The Picus Complete Security Validation Platform simulates real-world threats to continuously validate, measure and enhance the effectiveness of organizations' cyber defenses. The platform bolsters cyber resilience by identifying threat prevention and detection gaps, supplying actionable mitigation recommendations, and by facilitating a more proactive and threat-centric approach to security.

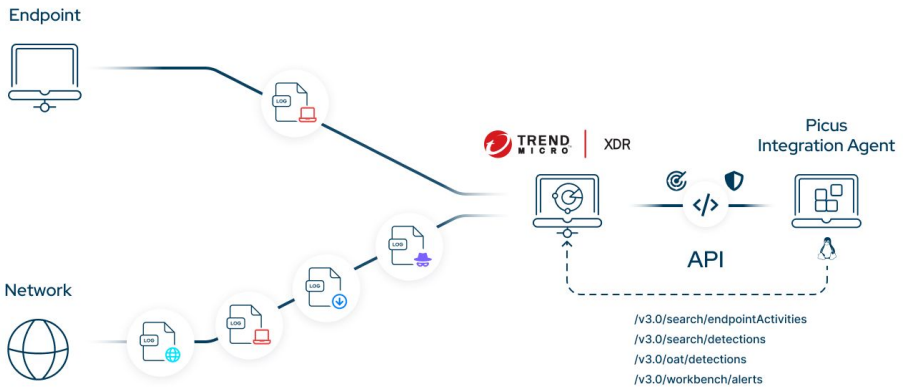
Why is security validation important?

- Controls don't perform out of the box and must be customized
- New threats mean that security tools can lose their effectiveness
- Infrastructure drift creates weaknesses that can go unaddressed
- Pen testing is vulnerability focused and quickly out of date
- Boards, auditors & insurers want evidence of security effectiveness

How It Works

To validate your existing Trend Micro Vision One XDR setup, follow these simple steps:

1. Install the Picus simulation agent on an endpoint protected with Trend Micro Vision One XDR.
2. Install the Picus integration agent and configure the API query parameters.
3. Simulate the threats you want to validate your setup with.
4. Analyse the insights about the level of protection and detection provided by your Trend Micro Vision One XDR configuration.
5. Mitigate the critical gaps based on the findings.



Integration Benefits

✔ Identifies missing, redundant and obsolete rulesets and watchlists.

✔ Identifies underperforming detections by measuring the time between security events and alert generation.

✔ Highlights behaviors that are detected but not blocked by prevention controls.

✔ Validates logs by ensures that logs contain the requisite level of data granularity.

✔Reveals delays in alerting and helps security analysts pinpoint issues such as storage availability, licensing, network outages, application conflicts, and others.

Target Persona

- SOC Managers
- Security Analysts
- Threat Hunters
- Incident Responders

Key Use Cases

Log Validation

By simulating real-world threats and analyzing the security logs captured on Trend Micro Vision One XDR, the Picus Platform uncovers if the right logs are collected and ensures the logs contain the requisite level of data granularity. The Picus Platform understands and prioritizes new data sources required to address logging gaps and help SOC teams to highlight behaviors that are detected but not blocked by prevention controls.

Alert Validation

The Picus Platform integrates with Trend Micro Vision One XDR to help security practitioners lower alert fatigue by eliminating low-quality alerts and false positives, and improving MTTD (mean time to detect) and MTTR (mean time to response) metrics.