XDR

SOLUTION BRIEF

MAXIMIZING EMAIL SECURITY WITH PICUS SECURITY AND SENTINELONE SINGULARITY XDR INTEGRATION

BUILD MORE ROBUST DEFENSES AND QUICKER DETECTION PROCESSES

INTRODUCTION

Endpoint Detection and Response (EDR) technologies have been a game-changer. Going beyond simple and fast-changing attack indicators, cyber security professionals can now build long-lasting detection policies against attack behaviors a.k.a. TTPs (techniques, tactics and procedures) utilizing rich endpoint telemetry. While the adoption of EDR has been relatively fast, the increasing sophistication of cyber-attacks and operational load create challenges in ensuring security tools remain effective at preventing, detecting, and responding to the latest threats.

Picus Security, the pioneer of Breach and Attack Simulation technology, and SentinelOne joined forces to make sure that SentinelOne Singularity XDR users can proactively update their security policies, achieve the best detection coverage with minimal operational effort and increase ROI. The Picus platform challenges and consequently applies advanced detection analytics queries on SentinelOne Singularity XDR to reveal unactivated and missing telemetry sources, and missing detections. The validation provided by The Picus Platform helps identify if EDR logging policies are set correctly and detection rules have the right scale and quality so that attacks are detected.

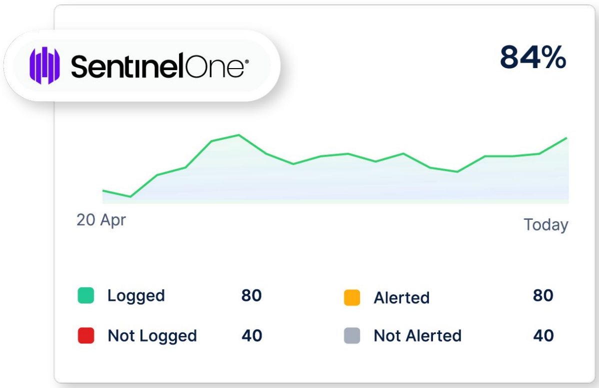
USE CASES

Improve Attack Readiness Visibility

The question “are we ready” often unsettles cyber security professionals as threats evolve and news of breaches become more frequent. Challenges around identifying the most relevant adversarial activities, business continuity, finding reliable test tools, and crafting threat samples make it difficult to establish if defenses are ready against new potential attacks. Offering the most extensive curated threat library in its field, the Picus Platform continuously challenges SentinelOne EDR with over 3,500 threats (and 18k+ actions) and custom-built scenarios. It identifies detection gaps and answers questions on readiness for SentinelOne EDR users with an intuitive UI effortlessly. Rich reporting features of The Picus Platform enable security teams to demonstrate the value of SentinelOne EDR.

Achieve Better Detection Rates and Faster Response Times by Adding Purple Teaming Capabilities

The integration between Picus and SentinelOne platforms ties internal and external risk factors together, aligns offense and defense teams, enables proactive Secops and SOC practices, and establishes a purple teaming capability. The Picus platform offers not only an innovative Breach and Attack Simulation technology but also a set of rich automation features and mitigation insights, whether it is in the form of telemetry enhancement or a new SentinelOne rule. Combination of this rich set of features and content helps security practitioners lower alert fatigue with automation improving MTTD (mean time to detect) and MTTR (mean time to response) metrics.



Operationalize MITRE ATT&CK Matrix to Achieve Metrics-Driven Operations

MITRE ATT&CK matrix for Enterprise has become the de facto knowledge base to understand adversarial behaviors and how criminal actors chain them together to launch sophisticated attacks. By mapping gaps and coverage findings for both security events and detections to MITRE ATT&CK, The Picus Platform elevates this knowledge base to a measurement baseline and helps SentinelOne Singularity XDR customers to run their operations with relevant and impactful success metrics.

ABOUT PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Complete Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, our people and technology empower customers worldwide to be threat-centric and proactive.

Test Your Defenses Against the Latest Threats

START FREE TRIAL

Gartner peerinsights™

4.9 / 5*

*average score at time of press in January 2023

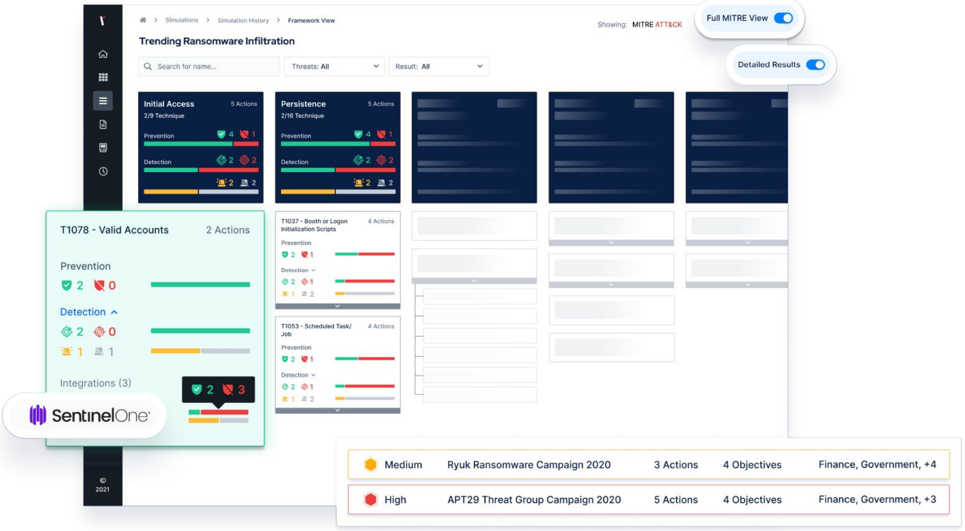
www.picussecurity.com

picussecurity

THE PICUS PLATFORM

The Picus Complete Security Validation Platform is built on an innovative Breach and Attack Simulation technology. The platform can run real-world simulations in production networks across email, endpoint and network attack vectors, utilizing Picus Labs' curated threat library. Picus is easy to deploy and supports cloud, on-premise and hybrid networks. It offers an intuitive user interface with advanced reporting capabilities.

Picus Labs is Picus Security's research division. It employs Red Team and Blue Team engineers who work as Picus customers' extended army of security analysts. Picus analysts have long years of malware analysis, ethical hacking, SOC engineering, incident response, threat hunting, detection engineering, and SOC Management experiences. Picus Labs collects threat intelligence from over 20 sources, analyzes malicious web activity, develops attack samples, and scans state-of-the-art defense technologies to offer the most effective mitigation content and guidance available.



Medium	Ryuk Ransomware Campaign 2020	3 Actions	4 Objectives	Finance, Government, +4
High	APT29 Threat Group Campaign 2020	5 Actions	4 Objectives	Finance, Government, +3

SENTINELONE SINGULARITY XDR INTEGRATION OVERVIEW

Based on seamless API-based integration, Picus Complete Security Control Validation Platform can become a SentinelOne user's de-facto validation tool. The integration reveals policy update requirements with a threat-centric perspective in relation to data generation settings on SentinelOne Singularity XDR. Thanks to the continuous attack simulation and analysis features, the integration provides trend analysis on security posture, historical and segment-based comparisons, MITRE ATT&CK Enterprise mapping, and other usability features. The integration also reveals delays in alerting and helps security analysts pinpoint issues such as storage availability, licensing, network outages, application conflicts, and others.

Enabling integration is straightforward as agents are lightweight and work on standard virtual environments. Customers need to install only one agent for the entire endpoint golden image sets. Once the agent is set up and given access, it starts querying the designated machine with SentinelOne running on it. The agent contains a proprietary list of threat attributes called a "keyword dictionary". Continually updated keyword dictionary guides detection analytics process in identifying missing adversarial behaviors with 100% accuracy.