Italian University Gains a “Panorama” View of Overall Risk with Rapid7 InsightIDR

Gaetano Pisano, network and security administrator at Universita’ degli Studi di Palermo in Siciliy, Italy, knows what it’s like to monitor a large environment with a small team. To help him do his job effectively, he’s turned to the cloud-based power of InsightIDR, Rapid7’s incident detection and response solution, and InsightVM, the evolution of Rapid7’s leading vulnerability management solution Nexpose. Now, he and his team are able to monitor hundreds of thousands of assets, gaining a “panorama” of all their vulnerabilities and their overall risk. In this Q&A, he discusses his program’s success in more detail. ►►►

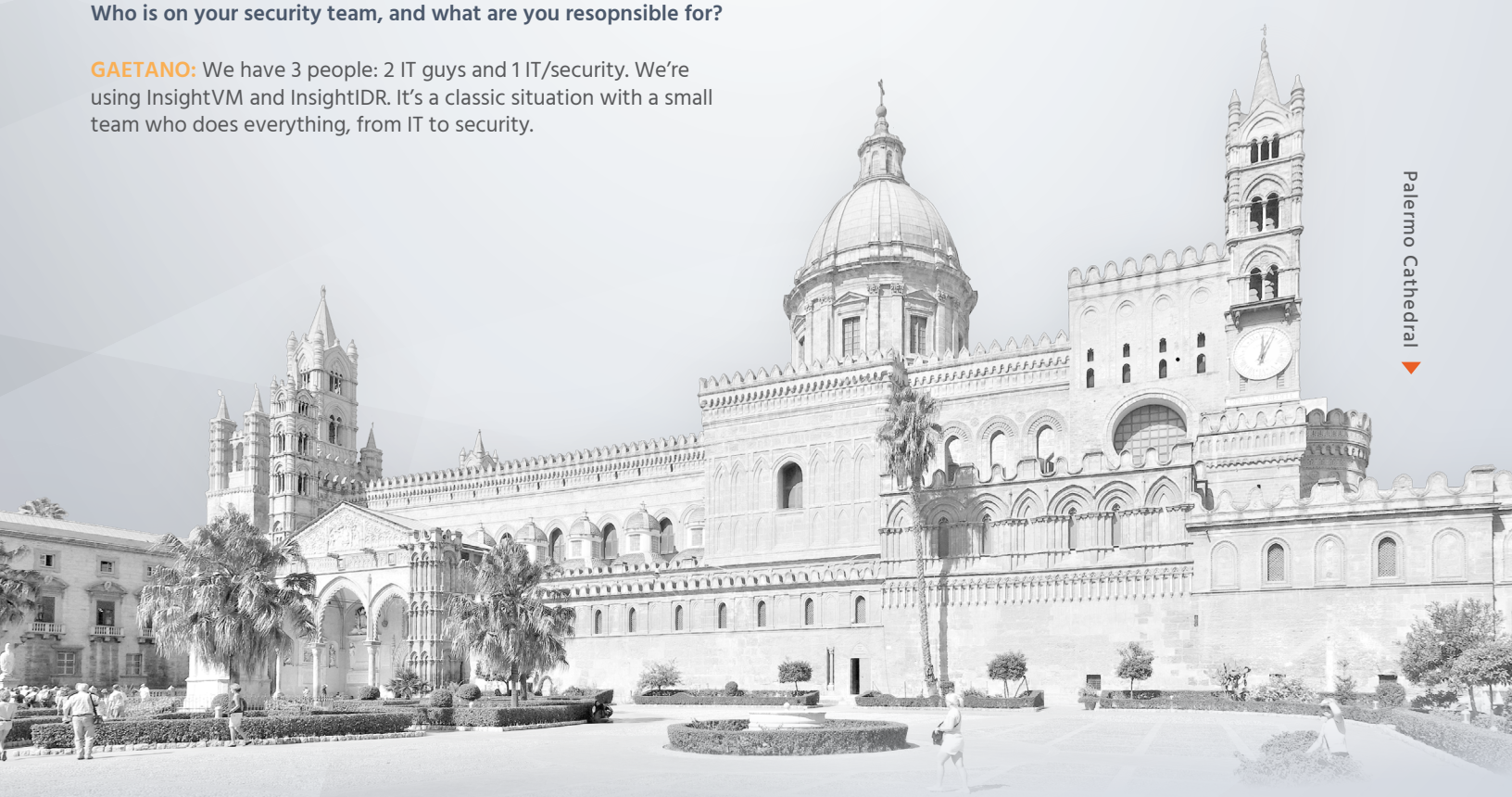
Tell us about Universita’ degli Studi di Palermo.

GAETANO: We have over 42,000 students and 3,600 employees (professors and others). It is part of the 10 largest universities in Italy. We rank 6th among the 10 for a variety of factors, such as: the services offered to students, the paid scholarships, the facilities available, the computerization and digital services offered, and the degree of “internationalization.”

COMPANY: Universita’ degli Studi di Palermo
SIZE: 3,600 employees
INDUSTRY: Higher Education
PRODUCTS: InsightIDR, InsightVM (previously Nexpose)

Who is on your security team, and what are you resopnsible for?

GAETANO: We have 3 people: 2 IT guys and 1 IT/security. We’re using InsightVM and InsightIDR. It’s a classic situation with a small team who does everything, from IT to security.



Palermo Cathedral

> After deploying InsightIDR, we no longer needed to query individual syslog servers to find answers.

Tell us about the environment you're monitoring.

GAETANO: We are responsible for hundreds of thousands of assets across the university. This also includes monitoring a transient, tricky class of devices to manage: our students' assets.

How do vulnerability management and incident response fit into your business and security strategy?

GAETANO: We wanted the ability to use one query to search across multiple services. In the past, we had to query each single server separately. We also wanted a "panorama" of all the vulnerabilities and visibility into overall risk and exposed services. I like being able to use Rapid7 Project Sonar data to confirm which university assets are truly exposed to the outside Internet.

What security challenges was the University facing? What problems were you trying to solve?

GAETANO: We needed to collect and retain our logs in a secure location to meet compliance, and we wanted to answer questions with that data. After deploying InsightIDR, we no longer needed to query individual syslog servers to find answers. We also needed flexible visibility into a range of operating systems, ranging from Windows, Mac and Linux to iOS, Android, and Windows phones.

Why did you choose Rapid7?

GAETANO: We'd heard of you online in a hacker forum called Cybrary (https://www.cybrary.it/forums/). We then found Nexpose and InsightIDR to be easy to use and configure.

What tools were you using before Rapid7?

GAETANO: Before InsightIDR, we were using Snort and AlienVault. Before Nexpose we were using OpenVas (open source).

InsightIDR

What was your process for investigating incidents prior to purchasing InsightIDR?

GAETANO: The products we used before were Snort and AlienVault OSSIM. Searching through logs in InsightIDR with the Log Entry Query Language (LEQL) is much easier and intuitive than with AlienVault. InsightIDR provides statistical data/queries that AlienVault doesn't, and comes with a lot more out-of-the-box value.

InsightIDR centralizes University log data in a secure cloud architecture. Are you satisfied with the ways InsightIDR gives you access to that data (i.e. log search, dashboards, and insight into user behavior)?

GAETANO: We're very happy with the speed of search, and the quality and clearness of the dashboards. The dashboards are very intuitive—I like that they are concise and contain only the info I want.

How does InsightIDR fit into your SIEM strategy?

GAETANO: We use InsightIDR for centralized log management, search, and data visualization. We can then monitor general activity, as well as traffic peaks on user endpoints. After identifying these anomalies, we can then decide if it's worth investigating or not. One day while investigating a traffic peak, we found one machine affected by SYN flooding that was originated by a compromised device.

What kind of incidents has InsightIDR detected so far?

GAETANO: The product detected malware traffic, infiltration, and persistence. It detected SYN flooding on one occasion, and in general it gives the ability to investigate peaks of activity and personalized queries to check for things like WannaCry, for example.

Are there any product-specific anecdotes you'd like to share?

GAETANO: Yes! One day our backup site went down due to high temperature (we are in Sicily, Italy), but we didn't have any issue with log storage thanks to InsightIDR and the fact that it centralizes our data in a secure cloud architecture.

How would you sum up the benefits of InsightIDR for your organization?

GAETANO: It allows us to correlate and interrogate logs from data sources across our network. We like the fact that InsightIDR securely stores our logs in the cloud at a good price. The product is easy to use, and out of the box, comes with many behavior detections, queries, and dashboards.

What's next for the University of Palermo and Rapid7?

GAETANO: In the future, we'll add threat intelligence from our Intrusion Detection System (IDS) into InsightIDR, and will look at using the included Insight Agent for endpoint data collection and detection. Also, we just moved from Nexpose to InsightVM and are quite impressed. The dashboards and detailed work put into this new release really blows us away.