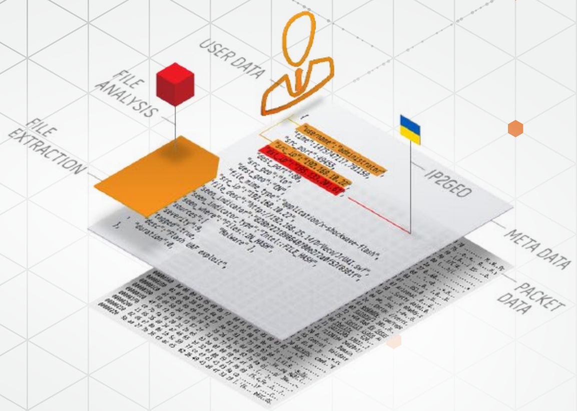
packetsled

packetsled.com
+1 (858) 225-2352

NETWORK VISIBILITY AUTOMATED INVESTIGATION ADVANCED THREAT HUNTING

Built by practitioners for practitioners, PacketSled provides automated network insight for risk management.

Pairing the immutable truth of wire data with the domain knowledge of your organization and enrichment from a virtually unlimited number of sources gives your security team the ability to quickly sort the signal from the noise and focus on real security incidents.



AUTOMATE NETWORK INSIGHT TO DECREASE RISK

Instrumental to any security team's success is the ability to encode knowledge specific to the organization into the security process and automate as many response activities as possible.

PacketSled's IRES (Incident Response Expert System) automatically follows the path of an attacker, mapping their activities to kill chain stages, so that your team can stop threats before they become incidents.

ENRICHED NETWORK DATA PROVIDES ULTIMATE CLARITY

PacketSled is the source of truth for every activity on the network, automatically fusing application data with file, user and endpoint context. This unique strategy enables your security team to gain unparalleled visibility into the behavioral risk of entities on the network.

SEARCH LIKE YOU THINK

LAST 3 DAYS DNS query like anomaly_patterns

HUNTING & INVESTIGATION BACKED BY UNPARALLELED HISTORY

Natural language queries enable security teams to search like they think and hunt threats across all observed data in seconds, whether an event happened five minutes ago or five months ago.

Interactive Visualizations give users the ability to see and drill into the relationships between threats and the evidence that supports them.

Continuous Monitoring provides the ability to detect and alert on previously undiscovered threats in your environment as new intelligence emerges and continually monitor your network risk profile.

Democratizing expert capabilities to prevent, detect, and respond to advanced threats.

Deploy Software Based Sensors in 15 Minutes | Cloud or On-Premise Deployment

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

SC MAGAZINE FOR IT SECURITY PROFESSIONALS ★★★★★

TechCrunch

Gartner.

CRN

packetsled

packetsled.com
+1 (858) 225-2352

NETWORK VISIBILITY AUTOMATED INVESTIGATION ADVANCED THREAT HUNTING

CASE STUDY

WHY THE CITY OF SAN DIEGO USES PACKETSLED TO GAIN DEEP VISIBILITY INTO ITS SMART CITY NETWORK

The City of SAN DIEGO

"My mission includes creating a "risk aware" culture and PacketSled is one of our go-to partner's provider in maintaining that. One of the great things about PacketSled is that I don't need to pay to add a sensor. In about 15 minutes, I can add visibility with only a few clicks. The future of security is the cloud software stack, and PacketSled has it wired."

-- Gary Hayslip
Deputy Director and CISO
City of San Diego

Overview:

As the eighth most populous city in the U.S., San Diego is home to 1.37 million people and 51,000 tech professionals. In 2015, San Diego was the only city selected in North America by National Geographic as a "World Smart City," which defined it as "one of the most forward-thinking cities across the globe." All of that attention yields pressure for the city of San Diego to secure its robust network that includes 5 petabytes of data across more than 40 agencies, including the Mayor and City Council. Securing information resources across a city that runs 24x7x365 is a responsibility that is taken very seriously and why Deputy Director and CISO Gary Hayslip chose PacketSled to help secure what he calls "a city environment in a constant state of change."

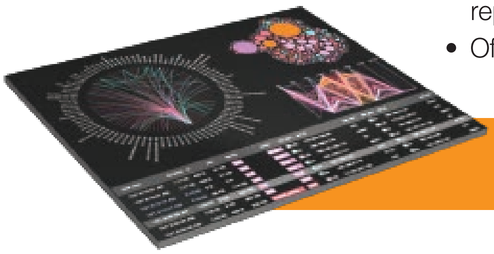
Challenge:

Understanding the City of San Diego's networks and how they are used by stakeholders was essential in creating an effective cyber security program. Aside from the 1.5 million external users that include San Diego citizens, the enterprise also includes more than 11,000 city employees and another 1,000 municipal employees of third party agencies. The City of San Diego is also connected to the Department of Homeland Security (DHS), municipal parks, and other attractive targets where a network break-in can cause major disruptions - from police cars and utilities to water treatment facilities, citywide resources are at risk if sophisticated controls are not in place. Without accurate visibility in such a complex environment, ongoing threat response can be adversely affected, and necessary action muted. In addition, the City of San Diego must comply with PCI-DSS for the handling of credit card payment data, HIPAA with respect to health data as it pertains to the records of city employees, residents of the city, and, various securities compliance regulations such as municipal bonds.

Solution:

Hayslip selected PacketSled, a cloud based platform that enables deep network visibility, continuous monitoring, automated investigations and incident response capabilities to secure its complex network. PacketSled helped the City of San Diego achieve several goals by:

- Providing a real-time view of the attack cycle that is ongoing within the enterprise network including full context of threats;
- Reducing the risk exposure to the city's enterprise by decreasing mean-time response, by increasing the fidelity of forensic data
- Offering the ability to automatically assess file payloads as they cross the wire, knowing immediately what resources are potentially affected by a specific attack;
- Providing full automation of the incident response process, which removed the burden of repeating similar investigations from the SOC team; and finally
- Offering near-zero false positive rate on detections.



View the Full Case Study at **packetsled.com**

Democratizing expert capabilities to know, prevent, detect, and respond to advanced threats.