PACKETVIPER®

Use Case

Optimizing SIEM & SOC with Deception360

Reduce Unwanted Noise and False Positives

The Challenge to SIEM Success: Complexity

Successfully deploying a SIEM is a complex task. That complexity is amplified by unmanageable noise from within the network and from skyrocketing volumes of global IP traffic. With SIEM vendors who have volumetric pricing models this can drastically increase subscription/license related costs. This struggle plagues security operations in organizations of all sizes and is a root cause problem.

Deception360: Removing the noise

As firewalls have evolved in their processing of application layer inspections, the epidemic of rising global IP traffic volume has made it less practical and secure to perform these deep packet inspections as a first line of defense. The deep packet inspection process within the firewall cannot afford to be cluttered with illegitimate traffic that a business has no use for.

Deception360 attracts threats, deceives them to gain new intelligence which can be applied at wire-speed. The solution solves the challenges of static perimeters in firewalls and creates a dynamic perimeter that can automatically change the access rules around any port or service and rotate them. This improves the threat identification process, lowers false positives and reduces alerting to security teams.

How it works

The Deception360 approach continually deceives attackers, gathers intelligence on threats and applies that intelligence to strengthen defense in a consistent and automated fashion. This greatly improves the performance of firewalls, IDS/IPS and SIEM solutions. Deploying Deception360 into a layered security approach provides a practical and cost-effective means to proactively strengthen cybersecurity.

With ‘point & click’ simplicity, Deception360 at a network boundary enables network obfuscation and very precisely reduces IP traffic volumes. This is done through a combination of deception and layered filtering approach that includes the ability to geo-target and perform precise filtering based on business intelligence, threat intelligence and customer rules, both inbound and outbound, at the port level. Deployment options include on-premise or in the cloud. Deception360 sits inline as an undetectable bridge at the perimeter of the network, as well as within segments and at other key network transition points throughout the network.

Deception360

Once illegitimate IP traffic volumes are reduced, network transparency is greatly improved and logs, alerts are streamlined across the network. Data quality is improved within the SIEM and SOC teams can check and remediate a much higher percentage of alerts.

Measurable security outcomes

Removing illegitimate IP traffic from the network without taxing the resources of the firewall, NGFW, IDS/IPS is one of the most proactive, cost-effective and impactful network security moves that one can make today. Measurable benefits include:

- Reduction in IP traffic
- Reduction in logs and alerts
- Reduced SIEM licensing costs
- Reduction in SPAM messaging
- Savings from deferred upgrades
- Bandwidth savings

About PacketViper

PacketViper has transformative and trusted cybersecurity solutions for organizations seeking better security outcomes across their converging OT & IT networks. Packetviper customers cover multiple public and private sector industries.