ONPAGE

SOME MESSAGES CANNOT WAIT

Improve Your Security With Threat Intelligence

Purpose of eBook

This eBook provides insight into threat intelligence and how it helps organizations avert security attacks. The document offers information about the benefits of threat intelligence and why organizations need to solidify their security policies or practices.

Turn the page to find out more. →

What’s Threat Intelligence?

Threat intelligence is the process of making raw data actionable. It’s the ability to convert attack data points into valuable insights, providing information about malicious activities and threats. Security teams use threat intelligence to identify system weak points and address them to avert costly cyberattacks.

Sources of Threat Intelligence

Security teams gather threat intelligence from a variety of sources. These include, but aren’t limited to, threat intelligence feeds, vulnerability databases and whitepapers or reports produced by trusted organizations.

On the other hand, raw threat data is retrieved from nation-state or NGO policies and expert news.

Best Practices

Incorporating threat intelligence into security practices isn’t a daunting task. It’s made simple with four best practices, including:

- Using intelligence proactively
- Integrating threat intelligence with existing security tools
- Using threat intelligence to reduce alert fatigue
- Combining threat intelligence with threat hunting

Using Intelligence Proactively

Threat intelligence is to be used as a guide for security operations. It identifies system vulnerabilities before an attack occurs.

Intelligence provides guidance on how to (1) limit permissions, (2) set up access controls to block attacks and (3) identify patches.

Threat Intelligence and Security Tools

Incorporate threat intelligence into automated systems and use it to define suspicious events or patterns of behavior.

This way, security teams can enhance their existing tools, ensuring that attacks are avoided.

Reducing Alert Fatigue

Alert fatigue is when security teams stop responding to alerts effectively or at all. This is caused by an overflow of alerts that don’t provide context into event severity.

Fortunately, threat intelligence sorts through alerts and lowers the priority of less relevant notifications. This reduces alert noise, ensuring that high-priority situations are addressed promptly.

Combining Threat Intelligence With Threat Hunting

Threat hunting is the process of proactively searching for threats that have bypassed security measures. When threat hunting, security analysts use threat intelligence to narrow the field of their search. Additionally, threat intelligence is the basis from which to begin a "threat hunt."

Where OnPage Comes in

OnPage provides [on-call rotations and escalations](). Web console administrators can select or task engineers, while creating “turns” if the first person is unavailable. This helps eliminate engineer burnout. OnPage also provides distinguishable high-priority alerts. Essentially, security teams will always know the severity of alerts.

Try for FREE

ONPAGE

SOME MESSAGES CANNOT WAIT

Try for FREE

OnPage's award-winning incident alert management system for IT, MSP and healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. OnPage enables organizations to get the most out of their digital investments, so that sensors, monitoring systems and people have a reliable way to escalate urgent notifications to the right person immediately.

OnPage's escalation, redundancy and scheduling features make the system infinitely more reliable and secure than emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response times.

Whether to minimize IT infrastructure downtime or to reduce the response time of healthcare providers in life and death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notifications needs.

For more information, visit www.onpage.com or contact the company at sales@onpagecorp.com or at (781) 916-0040.