# Arctic Security

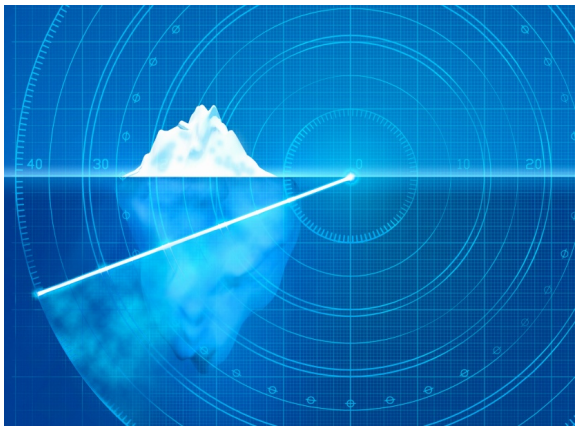
## EARLY WARNING SERVICE

### Discover and fix cyber security issues before harm is done!

There is a wealth of valuable external security information that is actionable for IT teams but not easily accessible. It is often too expensive for individual enterprises to acquire the data and cumbersome to filter out what is not relevant. Simultaneously, skilled cybersecurity professionals are a scarce resource whose efforts should be directed to where they can be most effective.

### Early Warning Service (EWS)

EWS leans on Arctic Security's experience working with national cybersecurity authorities in multiple countries, providing a platform for delivering security notifications to critical infrastructure. Those services have had a tremendous impact on the security of the recipients. Arctic Security now offers a commercial service that provides information on compromised and vulnerable services in your network, based on data available on the internet. EWS is an affordable service for organizations of all sizes to detect and fix security problems quickly.



Democratizing access to this information resource is beneficial for companies. EWS has been shown to reduce the time-to-discovery for compromised systems and vulnerable services. The notifications have warned about significant future security compromises before they occurred. They are digestible by IT professionals, helping organizations to improve security with the current staff. EWS uses high-quality data sources, which in a six-month study with a customer had false positive rate of less than 2 percent.

> *"This is a 24/7 job, and you feel better if there is somebody watching it. I would love to have a full-time network security person who did nothing but security, but for financial reasons that is not available. The service is invaluable to us, and that's personal as well as business. It lets me rest much better at night."*
>
> *– CIO of a private college*

EWS expands on the range of data available to you from authorities and provides a notification service that tracks incidents affecting your company's assets across national borders. EWS service is available as a monthly subscription, directly from Arctic Security and selected partners.

**Subscribe, register your asset information with Arctic Security, and receive timely notifications of your organization's security issues. They are already visible to the internet; you should see them too.**

# Arctic Security

An Early Warning service is beneficial for enterprises of all levels of security maturity. The service has a low entry barrier and a low price point compared to many other security services. That makes it particularly well suited for budget-constrained companies beginning to invest in cybersecurity. Knowing about the current issues is a powerful aid for decisions on other security investments. EWS helps to spot gaps in your understanding of the network and what may be going on without the IT staff's knowledge.

Many cybersecurity services require you to have reached a certain level of maturity in managing security issues. In contrast, Early Warning Service notifications can be consumed by IT professionals without extensive security training. Acting on the notifications serves to sharpen the IT staff's skills in preparation for high impact incidents in the future.

The EWS notifications help you to catch incidents that have passed through your current security measures. EWS tracks more than 80 vulnerable services and enables you to find and patch commonly overlooked cybersecurity issues. Still, it does not replace your existing security solutions, and can not catch all the incidents that may happen.

**A system with a reported compromise warrants immediate action from you. Combined with the vulnerable service notifications, EWS helps our customers to systematically improve their security processes to fix weaknesses that allow incidents to happen.**

The below table shows examples of different categories of data that are available through the service.

| Available EWS notification types | | |
|---|---|---|
| **Compromised systems** | **Vulnerable Systems** | **Open services** |
| • Infected hosts (e.g. bots communicating with sinkholes)<br>• Botnet infrastructure (e.g. command and control)<br>• Compromised systems that are serving malware<br>• Attacking IPs (Systems in your network attacking others)<br>• Sources of spam and phishing<br>• Defacements | • Services and systems with known vulnerabilities<br>• Services that enable use of weak crypto algorithms<br>• Services with expired x509 certificates<br>• Services facilitating amplification (DDOS) attacks<br>• Misconfigured servers | • Open database servers<br>• Open VPN and VNC servers<br>• Services that should not be exposed to internet |