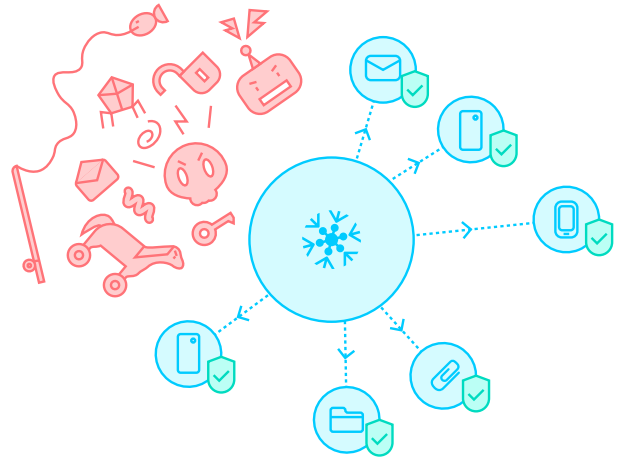




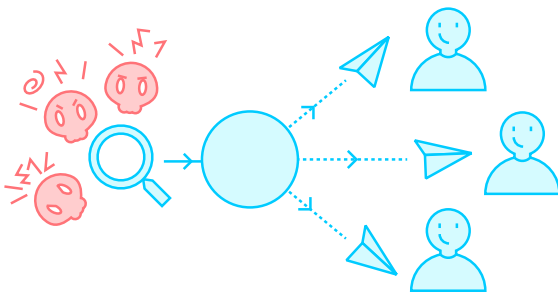
Arctic Security

Don't be alone
in cyber.



Get cyber threat information from the ones who know to the ones who need to know. Connect threat intelligence sharing organizations and enterprises with Arctic Hub and Arctic Node products.

Arctic Security has built its products based on years of experience operating in nationwide and nation-to-nation information sharing. Our headquarter is in Oulu, Finland and regional offices are in Helsinki and Singapore. We focus on actionable data about compromises and vulnerabilities and seek to automate the collection, harmonization, processing and distribution of that information.



Our mission is to help you get organized in cyber defense. We want to get both cyber security centers and security researchers connected with companies and help them share the critical threat information between each other.

In the heart of our approach there is a hub that receives and shares the essential threat information. A hub can typically be a national computer

emergency response team or a cyber security center or a managed security service provider. Or, in big organizations and companies a headquarters or other central unit can act as a hub and deliver the information to the other units.

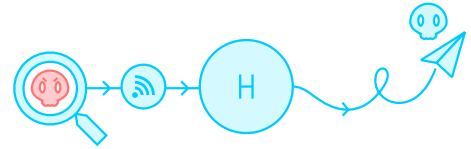
The role of the nodes is to collect the critical cyber threat information from their hub and act accordingly. For example, companies that are providing critical infrastructure can protect against the cyber threats reported to them by a national cyber security center.

Arctic Security Oy
www.arcticsecurity.com
contact@arcticsecurity.com
+358 20 743 100





HUB



Arctic Hub automates your cyber threat intelligence cycle

Arctic Hub enables threat intelligence sharing organizations to automate their cyber threat intelligence cycle where raw threat data is turned into actionable information. This ensures you get the threat information collected, harmonized and disseminated in a timely and effective manner.

Arctic Hub can be installed on your premises or on a dedicated cloud server, depending on your preference. When enabled, it collects and processes threat data from different information sources which can be commercial, open source or private. Arctic Hub allows you to share the collected information with your stakeholders through fine-grained controls. Information will be stored in the system for later access either as detailed observations or over-time statistics. Our customers always have full control over their data including its storage and processing without any dependency on Arctic Security.

AUTOMATED INFORMATION SHARING

- Threat data is automatically mapped to your customers based on their internet presence
- Choose which kind of information you want to share to each customer
- Your customers will get only the data that is relevant for them.
- You can choose to share these via email reports or through direct API access

SITUATIONAL AWARENESS

- See real-time information on the threats your customers have faced
- See the threats grouped by different factors such as type of customers, geographical area, type of malware or observation time
- Get situational awareness that helps you set up KPIs to follow up how your cyber security has improved over time

FEEDBACK FROM YOUR CUSTOMERS

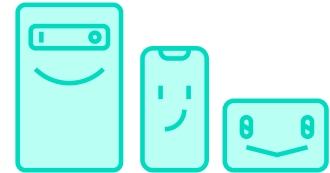
- See who of your customers have accessed the intelligence packages you have sent to them and when they have done that
- Understand how effective your threat information sharing is and if your customers find it useful

CONTROL YOUR THREAT INTELLIGENCE

- Arctic Hub can collect raw threat data from various threat feed providers
- Choose from the 150 feeds from 28 vendors of both commercial and open source data that are available out-of-the-box
- You are in control to choose which of them you want to activate in your use



NODE



Arctic Node lets you know what you need to fix

Arctic Node receives the threat information from Arctic Hub or other relevant sources and helps enterprises become more resilient in cyber security. You can use this information to make sure your network traffic, logs and security devices do not show indications of those threats. Integration to network security sensors helps you automate monitoring your network traffic.

Whenever you get information on critical issues in your own network you know what you need to fix immediately. To make the process even smoother you can automate some of the information flows by integrating Arctic Node to your existing security information and event management systems. Users of Arctic Node can also strengthen their defense by giving information back to their Hub. For example, you can validate the received data by confirming a sighting of a malware URL.

Arctic Node can be installed on your premises or on a dedicated cloud server, depending on your preference. The deployment is quick and user friendly. Our customers always have full control over their data including its storage and processing without any dependency on Arctic Security.

INTEGRATED WITH FEEDS AND PLATFORMS

- Arctic Node collects threat information directly from a cyber security center or other central operator using Arctic Hub
- Or, choose from close to 150 integrations to both commercial and open source feeds supported out-of-the-box
- You are in control to choose which of them you want to activate in your use. Or, you can even choose to integrate Arctic Node with your existing threat intelligence platform

INTEGRATED WITH SECURITY SENSORS AND SIEM

- Arctic Node can be integrated to security sensors and SIEM
- Sensors can automatically receive the latest cyber threat data in their use
- Sensors can alert you whenever suspicious traffic is detected
- By getting the up-to-date threat intelligence to your SIEM you get better analysis of your logs and find out the issues

INTEGRATED WITH INCIDENT RESPONSE PLATFORMS AND TICKETING

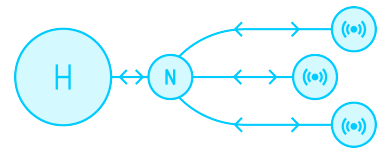
- Automate your information flows by integrating Arctic Node with your incident response platforms and ticketing systems

GET SITUATIONAL AWARENESS

- See real-time information on the threats you have faced
- Follow up on the trends how your cyber security has improved over time



SENSOR

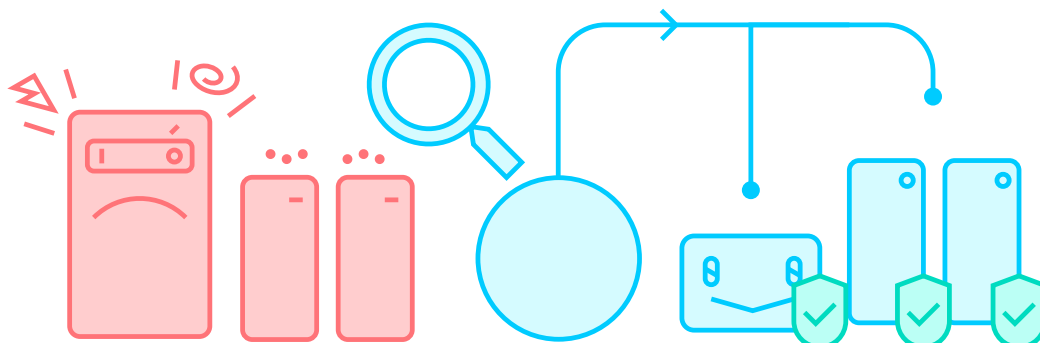


Arctic Sensor automates your network traffic monitoring

Arctic Sensor is an accessory to Arctic Node. It is a product for monitoring the outgoing network traffic of an organization. While monitoring the traffic Arctic Sensor continuously reads the threat intelligence data that it receives through Arctic Node. Thus, it can immediately alert back to Arctic Node if it detects outgoing internet traffic pointing to known malicious hosts, such as malware command and control servers or malware distribution sites.

Arctic Sensor is a software product which requires a dedicated physical hardware unit for network monitoring. It combines a high capacity sensor hardware together with the Arctic Security control system into a single deliverable solution which can be trivially integrated with Arctic Node. One Arctic Node instance can integrate with tens of Arctic Sensor units. There are two sizing options available for Arctic Sensor, one for the 1 Gbps line speed and the other for 100 Gbps.

Don't be alone in cyber.



Arctic Security Oy
www.arcticsecurity.com
contact@arcticsecurity.com
+358 20 743 100

