Arctic Security and Rugged Tooling join to provide

CYBER THREAT DETECTION FOR ENTERPRISES

Number of cyber threats grows as cyber criminals seek to gain financial benefits, for example from cryptocurrency mining malware. More and more malware sites are built each day. The threats cannot be prevented only with the help of user vigilance as certain malware bypasses user interaction completely.

Arctic Security and Rugged Tooling are developing together a solution that brings the cyber threat detection at the new level in enterprises. The co-developed solution includes Arctic Node threat intelligence product that has been integrated with Rugged Tooling cyber security sensor.

These two products work seamlessly together out-of-the-box and help monitor the internet traffic by detecting and alerting the user if traffic is pointing to any malware URL or criminal command and control server.

Reduce time to react to detected risks

Even with high end security measures, there is a possibility of cyber criminals getting in. Evasive malware has the ability to bypass firewalls and even sandboxes. Thus, while prevention is as important as ever, detection is a must. The integrated solution provides a comprehensive understanding of your security environment and real time insight into detected threats.

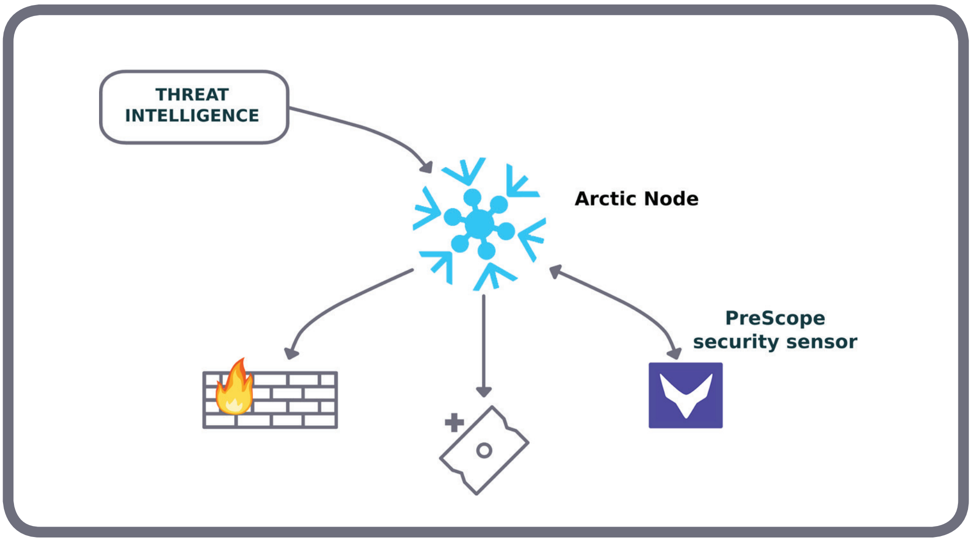
Arctic Security

RUGGED TOOLING

Arctic Node provides actionable threat intelligence

Arctic Node is a threat intelligence product targeted for enterprise use, developed by Arctic Security. It collects the cyber threat information from the various integrated sources that users can choose by themselves. Typically, Arctic Node is connected to Arctic Hub that is used by a national cyber security center or other threat intelligence sharing organization. Arctic Hub processes the raw threat data into customer specific threat intelligence packages. This way the information received by Arctic Node is immediately actionable and customized for the company's needs. Arctic Node users are always up-to-date on the cyber threats they are facing and thus, they know which issues they need to fix. For example, they may learn they have vulnerable services that could offer an opportunity for cyber attacks if not fixed.

Arctic Node can be integrated in many different security sensors, security information and event management systems, incident response platforms and ticketing systems. These integrations help improve the situational awareness and threat protection when threat intelligence is utilized effectively and timely throughout the organization.



PreScope sensor integration detects threats

Arctic Node can be used as a stand-alone product but the threat intelligence it provides can be put directly to use by integrating it with a cyber security sensor. Rugged Tooling and Arctic Security have co-developed the solution to provide organizations easily installed and cost efficient tools to expand their threat detection coverage.

The integrated sensors reduces reaction time by automating threat detection workflows to provide instant, actionable insight into the threats without extensive manual work. The sensor constantly reads the up-to-date threat intelligence provided by Arctic Node, monitors the traffic based on the threat information and upon detecting the threats, immediately alerts back to the user any traffic that points to any malware URL or criminal command and control servers.

Arctic Security

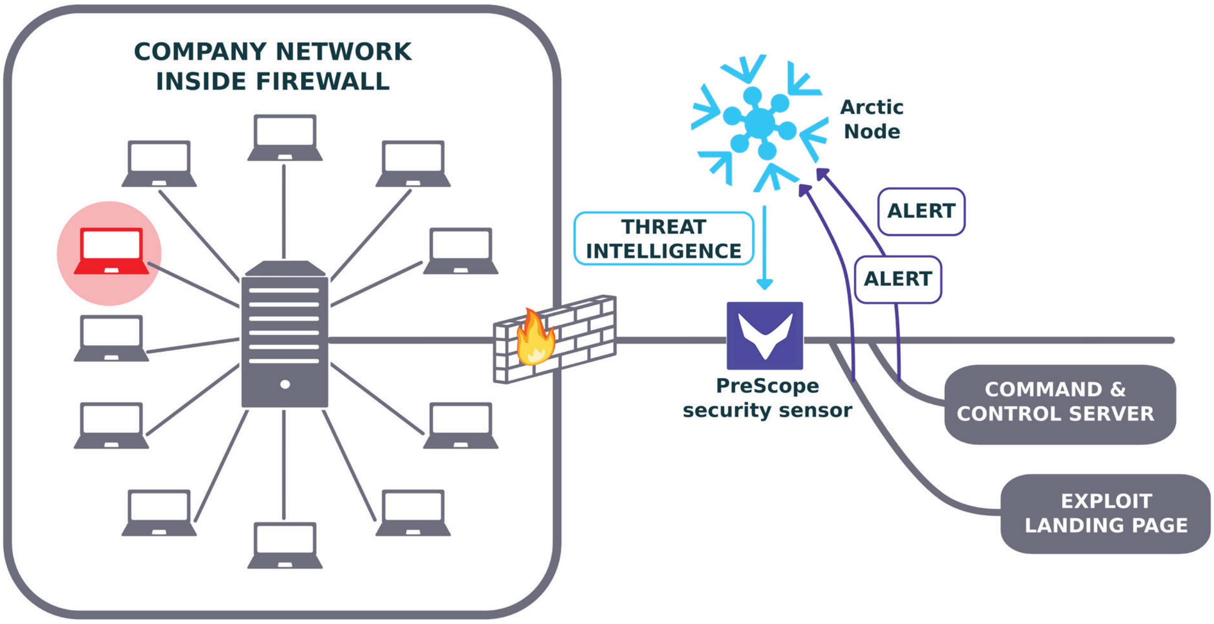
RUGGED TOOLING

Practical example: Stopping malware

The user of the red laptop goes to a website and sees a lucrative ad for ”Shoes 50% off”. He clicks on this ad to search for shoes, but instead, is forwarded into an exploit landing page. The page hosts malware that intends to infect the system of the user.

Luckily, Arctic Node is automatically collecting the latest threat intelligence from Arctic Hub. Thus, Node has already received information about this malware URL and has further submitted the address to the sensor to be monitored.

The sensor detects a known malware DNS name in the outgoing traffic and immediately sends an alert to the Node. The alert also triggers a full packet capture on the event, including also few moments before it to give the forensics team the possibility to understand what has happened.



Practical example: Uncovering malware infections

Despite efforts to prevent malware attacks, its continuous changes and evasion techniques may lead to a malware infection. Malware may be used to take control of the infected device, to use it in creation of denial of service attacks or to steal valuable information from the user. When active, the malware will communicate with the Command & Control server.

Node has the C&C server already blacklisted, and the sensor is already monitoring the traffic towards the server. Once the communication starts, the PreScope sensor will immediately detect it, and raise an alert to the Node and launch the packet capture on the event.

Improve your situational awareness

By deploying Arctic Node with the integrated PreScope sensor your organization gains improved visibility into cyber threats around you. Being able to detect the threats early gives you detailed insight into the circumstances leading to the infection, which allows the organization to learn and improve their defences for future attacks.

The threat intelligence provided by Arctic Node is tailored to your organizations, ensuring better situational awareness in your enterprise. The integrated, automated threat detection with PreScope sensor and reduces time and manual work needed to detect the threats in your network traffic.

Contact us

To learn more about how our joint solution can be deployed to best benefit your organization, contact us at either contact@arcticsecurity.com or sales@ruggedtooling.

Don’t be alone in cyber

www.arcticsecurity.com
contact@arcticsecurity.com

Ensuring robust and secure digital communication

www.ruggedtooling.com
sales@ruggedtooling.com