Addressing Insider Threats, Cyber Attacks & Data Security

How Simple Sharing Leads to Stress Reduction and Security Agility

A few years ago I asked a seasoned security practitioner what keeps him up at night? He quickly responded 'why does that IP address originating from China continue to ping my organization every day for the last 5 years'. Sharing threat intelligence today is starting to make a difference by shedding light on the malicious IPs, URLs, and hashes. The information available today is growing with ISAC and ISAOs enabling the vertical communities with free flowing threat intelligence combined with the growing open source and commercial feeds. Today if I asked this same person what keeps them up at night, I bet he would say he's constantly stressed that he is missing the threat campaign targeting his company and industry because tactics can now include changing IP addresses daily.

There are various ways of ingesting all of this shared threat intelligence, even free solutions. But sharing this information is not dynamic enough to achieve sustainable and agile security to counter the ever-changing threat landscape. The same characteristics that draw people to Banks are the ones that can help with this problem: personal focus, flexibility, community, and best fit recommendations.

Personalization – Focus on only the threats that are relevant to your organization and reduce the noise. Automate correlation to get results based on the technology of your organization and see which threats are the most important.

Flexibility – Threat campaigns change and there is no singular standard for sharing threat intelligence. Enable the ability to ingest both structured STIX/TAXII and other types with unstructured threat data from email and .pdf files. Have the ability to alter associated risk scoring as needed based on your expertise to reduce encountering false positives or false negatives.

Trusted Community – Augment your current threat program by creating your own trusted community with peers, affiliates, and vendors across your digitally connected ecosystem. Gain first sightings of indicators of compromise targeting your ecosystem, and develop your own hyper relevant community-driven threat intelligence feed source.

Recommendations – Leverage the ability to generate expert-driven security recommendations. Receive firewall and endpoint rule change information at your fingertips to proactively protect against high-risk threat indicators.

BrightPoint Sentinel changes the model for how organizations and industries can collectively prevent cyber attacks leveraging automation, machine-learning analytics and most importantly, non-attributed sharing of threat indicators. For the first time ever, BrightPoint Security Trusted CirclesTM facilitate the safe sharing of threats that are being seen from inside the virtual perimeters of organizations. From this hyper relevant threat information predictive insight is achieved to understand the looming threats and the threat trends that enable security teams to work together, across their industries or ecosystems, to proactively avert attacks before they can gain a foothold. Ask about a demo highlighting STIX/TAXII support and how BrightPoint Sentinel automates the curation and enrichment of threat indicators. Let us change your view about what a threat intelligence program should deliver.

BrightPoint Security transforms how organizations protect their expanding virtual security perimeters by providing immediate and predictive insight. Built on a platform independent of infrastructures and workflows with an open API to accommodate the breadth of today's security technology implementations. Gain unprecedented visibility into threat campaigns across digital ecosystems and industries.

Ajay Nigam
Senior Vice President

BrightPoint SECURITY

Contact Info
www.brightpointsecurity.com
650.946.1893

Ajay Nigam is the Senior Vice President of products at BrightPoint Security. Ajay has served in executive roles at CipherCloud, Marble Security, Symantec, and VeriSign. Ajay earned a BS Tech in Telecommunication from University of Jabalpur, and is a Fellow of Indian Institute of Telecom Engineers (FIETE) and the founding Co-Chair of O-Auth. BrightPoint Security delivers immediate predictive insight and prescriptive response to protect businesses from cyber threats. BrightPoint enables secure community-based threat intelligence sharing to achieve the most relevant visibility and awareness of current and emerging threats across enterprises, their digital ecosystems and infrastructures. Venture backed, the company is headquartered in San Mateo, CA.