opentext™ | Cybersecurity

Data Sheet

Galaxy Threat Acceleration Program Plus (GTAP+)

Premium threat intelligence to empower ArcSight SecOps detection and response

Key Features

- Premium threat intelligence
- Plug and play SmartConnector
- Vetted intelligence
- ATT&CK and D3FEND

Key Benefits

- Simple to use
- Proactive defense
- High-fidelity alerts
- Built for ArcSight

Product Highlights

Your organization is under constant pressure to defend against cyber security threats, and unfortunately, this represents a real challenge to business outcomes in an increasingly digital world. Existing solutions compete to provide the latest and most exclusive information, but the sad reality is that trying to stay on top of all the latest threat intelligence feels like drinking from a firehose. Many companies are left with a wealth of information about threats and IOCs, but little to no information on where to start, how threats are affecting their business, or how to best defend their organizations.

OpenText™ Cybersecurity Galaxy Threat Acceleration Plus (GTAP+) is a premium threat intelligence feed specifically built for ArcSight Enterprise Security Manager by OpenText™. It incorporates insights from Galaxy's threat research network, and provides ArcSight customers with proactive defenses. It increases your coverage against modern threats and threat campaigns by providing visibility, reducing false positives, and automating threat response.

Galaxy's superior content facilitates out-of-the-box threat detection and response for ArcSight ESM, and powers advanced implementation of ATT&CK and D3FEND

countermeasures. It provides threat monitoring content that's always on and always up to date. It eliminates blind spots and helps stop breaches before they occur, packaged in a solution that can be installed and operational within minutes.

Key Benefits

Simple

Using GTAP+ is simple. By installing the plug and play SmartConnector, you'll gain immediate out-of-the-box access to detection and response content built specifically for ArcSight ESM. The installation is easy and takes a matter of minutes, and the immediate implementation of ArcSight rules and correlations means that engineers and analysts can save their time for other tasks.

Proactive

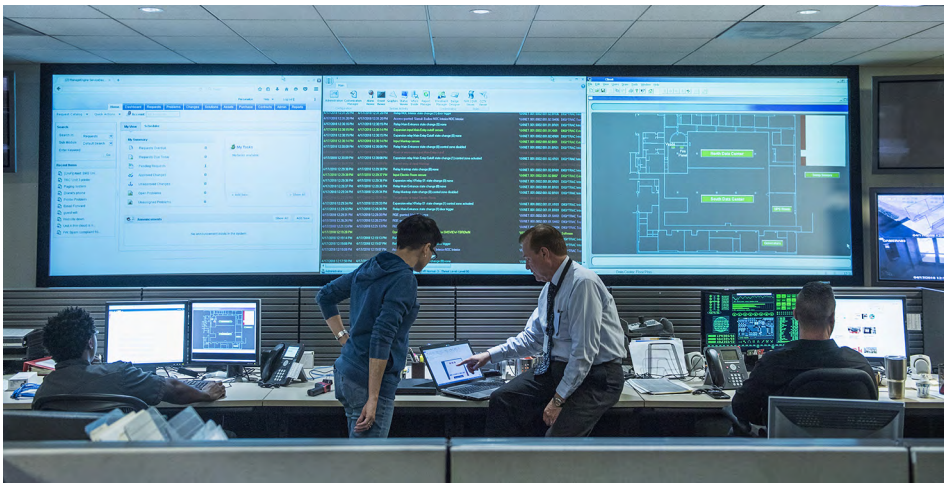
GTAP+ provides advanced implementation of MITRE's ATT&CK and D3FEND countermeasures to help build a proactive and resilient defense for your organization. With downloadable content from Galaxy, you'll be able to build strategic defenses for your organization based on your specific industry risk and threat landscape. With a more proactive and resilient defense, you'll be better equipped to stop breaches before they occur.

High-Fidelity

We understand that chasing down false positives wastes precious time and resources for your SecOps team. With Galaxy Threat Acceleration Program Plus, you'll focus your time on threats that actually matter to your organization. GTAP+ uses high-reputation indicators for IP addresses, hash values, email addresses, domain names and URLs. Our verified, human-vetted threat feed delivers quality over quantity, which allows analysts to devote their time to the threats that matter.

Built for ArcSight

Galaxy Threat Acceleration Program Plus was built specifically for the benefit of ArcSight users. It provides increased coverage of modern threats and threat campaigns with content pre-built for ArcSight's detection and response. GTAP+ threat intelligence feed directly integrates with ArcSight's real-time correlation, and provides coverage that's always on and always up to date.



Key Features

Premium Threat Intelligence

GTAP+ provides intelligence that is accurate, timely, and high-fidelity. Galaxy's global threat research network sources indicators of threats that are reliable, and in some cases GTAP+ provides information for APTs and 0-day threats even before the OSINT world knows about them. Packages of timely, technical details about new and innovative threats and attack campaigns help you understand more about the current threat landscape. Galaxy's unique perspective on the latest threats helps you make informed, risk-based decisions based on pertinent information for your industry, so you can develop the appropriate mitigation procedures for your defense.

Additional Intelligence Sources

- Partner global incident response
- Trusted public intelligence (OSINT, etc.)
- National CERT intel
- Dark web intelligence
- Industry sanctioned intelligence programs
- Trusted 3rd-party threat analysis
- Geopolitical intelligence
- Daily ThreatCon surveillance
- CyberRes sensory capabilities

Plug and Play SmartConnector

Installing and operating GTAP+ couldn't be any easier. Simply install the plug and play SmartConnector, and you'll immediately have access to threat detection and response content built specifically for ArcSight ESM. Connection to the premium feed means that your threat intelligence is always on and always up to date, which automatically refreshes every 30 minutes.

Vetted Intelligence

The Galaxy team maintains a high standard for the intelligence that makes it into the GTAP+ feed. In order to maintain the accuracy of IOCs, multiple APIs are used to triangulate, prioritize entries. A real-time algorithm is used to calculate confidence in each threat, and each entry is assigned a score. Each entry is checked to make sure it's not listed in the "safe lists", and entries are

also enriched with additional metadata such as malware name, type, and geolocation. Manual, vetting is also performed when curating indicators related to notable breaches and by our threat hunting team.

ATT&CK and D3FEND

We're arming ArcSight with special weaponry to turn it into a detection and response machine, regardless of your current SecOps maturity level. Galaxy's GTAP+ content automates the advanced implementation of ATT&CK and D3FEND countermeasures, which provides a strategic and proactive approach to security. This is like rocket fuel for ArcSight's detection and response engine, and will ultimately help you eliminate blind spots in your defense and stop breaches in their tracks.

Learn More

Register for an account at:
www.cyberresgalaxy.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000034-003 | O | 10/23 | © 2023 Open Text