Outmaneuver Your Adversaries with Intelligent SecOps

As the velocity, volume and variety of cyberthreats continue to grow, organizations face increasing risks of IP theft, sensitive data loss, compliance violations and high-cost remediation. The credibility of the security operations team is also at risk given the rapidly expanding attack surface and resource constraints. Cybersecurity analysts are often swamped with false positives which divert them from finding the real threats. It has become imperative for SOC operators to accelerate effective threat detection and response in order to minimize exposure time.

Intelligent SecOps at a Glance

Maximize Efficiency

Empower analysts to focus on what matters and cut down false positives while reducing mundane and low value-add tasks with process automation

Improve Effectiveness

Elevate detection accuracy with contextual insights while enabling fast and relevant actions with intelligently automated responses

Enhance Resilience

Adapt to changing threat landscape by evolving security posture with dynamic intelligence feeds, analytics and response process

Ponemon Institute's '2022 Study on Closing the IT Security Gap: Global' indicates that 30% of organizations consider themselves highly effective in keeping up with a constantly changing threat landscape and closing their organization's IT security gap. These high performing organizations are found to be more aware of the benefits of automation with 78% of them citing the most important benefit is the ability to find attacks before they do damage or gain persistence.

The timeless healthcare adage—"prevention is better than cure"—finds itself equally applicable in cybersecurity. In light of the ever-increasing attacks and the ever-challenging resource situation, it is crucial to adopt a highly efficient and effective approach for preemptive detection and response. The Ponemon study* also mentions that the top two benefits cited for using AI and advanced analytics are more efficient investigation and more effective security teams.

An AI powered 'Intelligent SOC' lets you to preempt, withstand and recover in less time by significantly increasing operational efficiency and effectiveness with accelerated real threat detection and response. An 'Intelligent SOC' should provide holistic situational awareness and streamline end-to-end processes.
Key enabling capabilities are:

- **ArcSight's 360° Analytics**—Given the plethora of threats (known and unknown), you need more than one arrow in your quiver. An analytics approach harnessing the collective power of real-time correlation (ArcSight ESM), behavioral analytics (ArcSight Intelligence) and big data analytics-based hunting (Arcsight Recon) minimizes blind spots. Different techniques are better suited to analyzing, for example, log events, user actions, and anomalous traffic. Working together, these analytics can more effectively address the entire kill

*The 2022 Study on Closing the IT Security Gap: Global, Ponemon Institute

“AI finds stealthy threats and makes security teams more effective and efficient.”

The 2022 Study on Closing the IT Security Gap: Global
Ponemon Institute, January 2022

Contact us at **CyberRes.com**
Like what you read? Share it.

chain by capturing an attack at different points in the chain of events that can start with reconnaissance by the attacker and extend to payload deployment and impact

- **Galaxy’s Advanced Threat Research**—Unlike regular threat intelligence, advanced threat research provides curated and contextually relevant insights. It focuses on attributes that are relevant to business such as Annualized Loss Exposure (ALE), industry, impact, activity, discoverability, and effectiveness. Another key aspect is how the information is fed into your SIEM. A fully integrated and automated feed will further contribute to efficiency.
- **ArcSight’s Native SOAR**—Exposure time is the sum of detection time and response time. To minimize exposure, detection and response must work hand in glove. SOAR should be an integral capability of a SIEM. SOAR should intelligently automate time consuming and mundane tasks, prioritize incidents, and take timely action on threats. Analysts’ productivity will get a boost with an Intuitive service desk enabling security investigations and responses to be carried out from a single pane of glass.

“ArcSight Intelligence found a successful authentication to a rarely used server, which attempted to access servers globally. Narrowed down to an administrator who was dismissed as a result, ArcSight Intelligence then spotted the same account trying to re-authenticate after the individual had been terminated. All attempts were identified and neutralized.”

Chief Information Security Officer
Large Healthcare Organization

CyberRes
A Micro Focus Line of Business