Intelligent SecOps Pitch Card

What can an Intelligent SecOps solution do?

Help you build an AI powered 'Intelligent SOC' so you can **preempt, withstand and recover in less time** by significantly increasing operational efficiency and effectiveness.

What problems does it address?

- **Talent Shortage–** Chronic lack of resources leads to high risks of oversight, fatigue and attrition
- **Attack surface expansion** – Threats outstrip strained resources, exacerbates resource problems, and increases exposure time.
- **Extended exposure time** - Slow detection and response leading to higher cost of remediation and unnecessarily high level of damages (e.g. IP theft, sensitive data loss, compliance violations. business disruptions), and credibility loss of security team.

What are the customer pain points?

- **Growing threats to business:** Cyber threats are becoming increasingly sophisticated and are impacting greater portions of the business value chain.
- **State-sponsored attacks**: Cyber campaigns funded by government actors to gain access to sensitive assets in order to gain a competitive advantage.
- **Multi-branch/agency complexity:** Branches or agencies separated by location, country, network infrastructure, or administrative organization, but requiring connectivity and security visibility.

What are the customer benefits?

- **Maximize efficiency -** Empower analysts to focus on what matters and cut down false positives and reduce mundane and low value-add tasks with process automation
- **Improve effectiveness**: . Improve detection accuracy with contextual insights and enable fast and relevant actions with intelligently automated responses.
- **Elevate Resilience**: Adapt to changing threat landscape by evolving security posture with dynamic intelligence feeds, analytics and response process

Buyer Profiles

a. Large enterprises
b. MSSPs
c. Government agencies

Roles

a. CISO
b. SOC executives with budget authority

Top Competitors

a. Splunk
b. IBM
c. Exabeam
d. Securonix
e. Microsoft

(Visit Enablement Central for competitive analyses & 2022 Gartner MQ for SIEM field response brief)

Intelligent SecOps

ArcSight and Galaxy are for security operators who need to efficiently and effectively protect their environments by enabling their SOC teams to accelerate real threat detection and response. Unlike other vendors, ArcSight and Galaxy provide holistic situational awareness and streamline end-to-end processes with fully integrated native SOAR and threat intelligence capabilities.

What are our main differentiators?

- **360° Analytics –** Harness the collective power of real-time correlation, behavioral analytics and hypothesis-based hunting to catch different threats.
- **Advanced Threat Research -** Automated feeds of curated and contextually relevant insights into SIEM
- **Native SOAR -** Out of the box fully integral capability of SIEM.

Discovery Questions: How to approach the discussion

1. What do you think about your current MTTD and MTTR?
2. Do you have any concerns about missed detections? If so, why do think the misses are happening?
3. If improvements are needed, what would those be?
4. Are there any barriers against reaching the improved state? If so, how do you plan to overcome those barriers?
5. What are you currently using for SIEM?
6. What are you currently using for SOAR?
7. How are your SIEM and SOAR integrated?
8. How well does your current solution address both known and unknown threats?
9. What do you think about the staff resource requirements?
10. What do you have in place for insider threat prevention?
11. What EDR solution do you use?
12. What threat intelligence solution do you use?
13. What has your experience been with your threat intelligence feeds?

Products for Intelligent SecOps?

- ArcSight – 360° analytics and native SOAR
  - ArcSight SaaS (behavioral analytics, log management and reporting, hypothesis-based threat hunting)
  - ArcSight ESM (real-time correlation)
  - ArcSight Intelligence (behavioral analytics)
  - ArcSight Recon (log management & reporting, hypothesis-based threat hunting)
- Galaxy – Advanced Threat Research
  - Galaxy Online (curated and contextual relevant threat insights)
  - GTAP+ (integrated Galaxy feeds into ArcSight)

Resources

- Sales Enablement Central