COMPETITIVE BATTLECARD

paloalto NETWORKS

COMPETITIVE PRODUCTS

AutoFocus: Contextual threat intelligence service leverages Unit 42 threat researchers.

Cortex XSOAR: Security Orchestration, Automation, and Response platform.

THEIR PRICING

AutoFocus and Cortex XSOAR pricing not listed publicly. Available for purchase via resellers including CDW.

THEIR MARKET PRESENCE

- 2018 Cybersecurity Gold Badge (company)
- 2019 Cybersecurity Best Analytics Silver award
- 2019 Canalys Cybersecurity Leadership award
- Strong industry recognition for next-generation firewall solutions
- No industry recognition for TIP or SOAR services/solutions

COMPANY FACTS

- Founded 2005
- Raised five rounds of funding totaling $65M
- Raised $260M in IPO on July 20, 2012
- +14% employee growth over 12 mos, mostly in engineering, IT, and sales
- Revenue: $3.4B (18% YOY growth)
- Employees: 8,014 (801 open positions)
- HQ: Santa Clara, CA

THEIR SALES TACTICS

- TIP services to embed threat intelligence into analyst's existing tools to speed investigation, prevention, and response.
- Crowdsourced intelligence from the industry's largest footprint of network, endpoint, and cloud intelligence sources.
- Threat intelligence repository offers visibility into real-world attacks sourced from 65K+ customers for 10+ years.
- Over 14 billion samples collected, 7 trillion artifacts analyzed, 3K hand-curated tags with adversary details.
- Cortex XSOAR unifies automation, case management, real-time collaboration, and threat intelligence management.
- Hundreds of SOAR playbooks for phishing prevention, IOC enrichment, vulnerability management, and cloud security.
- XSOAR has 400+ integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, and messaging systems
- Automated multi-source feed aggregation; granular indicator scoring and management; ML-driven virtual assistant.
- Focus on analyst time constraints and resource shortages by offering TIP services and SOAR unifying automation.

THEIR TARGET MARKET

- Primarily target small to medium businesses, MSSPs, and enterprise firms
- Focus on TIP services combined with a SOAR solution
- Offer XDR complementary solution
- Target gov, SLED, financial, healthcare, mfg, energy, retail
- TIP and SOAR are not priority solutions compared to firewall, etc.

STRENGTHS

- Won several awards for NGFW solutions and market leadership
- Crowdsourced intelligence from large industry aggregated sources
- Intelligence repository spans 65K+ customers and a decade
- TIP service uses Unit 42 global threat intelligence team & playbooks
- Has 3K tags with details about adversaries, campaigns, malicious behaviors, malware families, exploits, and techniques
- High customer praise for dashboard and interface.
- Customers include Sega, Telkom Indonesia
- Robust SOAR solution integrates with TIP services offering

THEIR WEAKNESSES

- Only offers TIP services, does not offer a complete TIP solution
- Analysts must rely on Palo Alto for all TIP intelligence and tools
- Threat intelligence repository limited to Palo Alto customers
- Lacks technical documentation details on specific threat types
- Limited customization and no custom fields available
- No threat intel collaboration or finished intelligence
- No brand protection or threat investigation
- No off the shelf support for automated real-time or historical/retrospective forensics
- No phishing analysis /sandbox, not cloud-native
- No ML to determine threat scores or reduce false positives

HOW WE SELL

HOW WE SELL

- 2019 Cyber Defense winner, SC Media 5-Star Rating, 2019 Cyber Security winner.
- Fast deployment via cloud, on-premise, AirGap. Plug-n-play APP store.
- Robust out-of-box integrations; developer SDK enables custom integrations.
- Highly accurate and automated machine learning (ML) scoring algorithm; uses 130+ public, private, and proprietary sources to reduce false-positives by 95%+.
- Enriches billions of meta data events; provides sandboxed threat detonation.
- Enables high accuracy detection of attacks via Domain Generation Algorithm (DGA) with 90%+ accuracy and contextual data: WHOIS, PassiveDNS, others.
- Lens uses Natural Language Processing (NLP) to auto-scan and identify threat data in web content, reducing time required to research and understand threats.
- Context-based intelligence; collaboration for ISAC/ISAO threat intel sharing.

WHY WE LOSE

- Customer desires threat intelligence services and does not need a full TIP solution.
- Anomali's usability, dashboarding, and UI aspects may be a concern for some prospects
- Firms with limited intelligence analysts or resources may prefer TIP services over a full TIP solution
- May convince customers that TIP services combined with a SOAR solution will meet all threat intelligence requirements
- May win account with the SOAR solution and upsell TIP services

OBJECTION HANDLING

Objection: Palo Alto claims to offer TIP services with a SOAR solution meet all threat intelligence requirements. What does ThreatStream offer?

We Respond…

- Palo Alto has an excellent SOAR solution but does not offer a full TIP solution. They only offer TIP services. This limits your threat intelligence feed sources, customization capabilities, and does not allow you to score indicators of compromise (IOCs). They may also pass through too many false positive alerts.
- Anomali's ThreatStream can easily integrate with almost any SOAR solution, but we also provide a far more robust rather than only a "lite" TIP solution.

Objection: Ponemon research says false positive alerts are now a primary concern. How does your false positive determination compare to Palo Alto?

We Respond…

- Palo Alto is only a service and unlike ThreatStream, they do not use machine learning algorithms to provide threat and risk scores. We offer more advanced context-based intelligence and higher accuracy, which is why our customers report over 95% false positive reduction rates.
- New State Civil Codes (e.g; NYDFS) require proving that Personally Identifiable Information (PII) was not exposed during a threat, which requires disproving false positive alerts. Anomali's automated ML scoring algorithm reduces false positives by 95%+, which lowers risks and security team/analyst efforts and time.

Objection: Palo Alto's AutoFocus appears to offer complete threat intelligence capabilities. How does that compare to Anaomali's ThreatStream?

We Respond…

- Palo Alto's AutoFocus is not a TIP solution, but only a service, so they lack threat scoring as well as Natural Language Processing (NLP) capability to scan web pages. ThreatStream offers threat scoring and reduces research time to understand threats by auto-scanning and identifying threat data in web content.

Objection: Palo Alto's TIP service uses their Unit 42 threat intelligence team and data from 65K customers. How does that compare to ThreatStream's

We Respond…

- Palo Alto only offers a "TIP lite" solution as a service with limited intelligence threat feed sources. ThreatStream has 130+ public, private, and proprietary sources. Given recent threat escalations, most firms view a limited intelligence feeds as high risk and prefer a full TIP solution. ThreatStream uses a highly accurate machine learning algorithm to score indicators of compromise (IOCs) to rationalize multiple threat data sources into a single repository and automatically normalize, de-duplicate, remove false positives, and enrich threat data. Palo Alto does not have the additional feeds, Lens NLP, or as robust integrations, which may expose you to data breaches, lawsuits, and fines.

WINS

BLACKHAWK NETWORK

- Single dashboard, threat intelligence feed consolidation
- Seamless SIEM integration
- Sandbox to detonate payloads
- Threat analysis, response times
- Reduced false positives by 95%+

Bank of Hope

- 5 to 1 dashboard consolidation
- 90% threat analysis time reduction
- Visibility: additional analysis feeds

Fed Sys Integrator

- Consolidate threat intel data
- Contextualize intel
- Reliability & pertinence
- Focus & action info