VERSATILITY

Versa Behavioral Insights - Threat Hunting and AI Insights

Siddhant ‘Sid’ Ramaswamy

Director, Product Management

Today's SASE Operations Challenges

Alert Fatigue

Too many blind spots and threats buried under noise

Lack of Visibility

Cost and inefficiencies to access and correlate across different silos

Unsophisticated Threat Detection

Limited coverage for constantly changing threat landscape

Operational Overhead

Increased tool sprawl leading to increased operational costs

Rise in Threat Vectors

Increased attack surface and complexity

Automation Post Hoc

Insufficient automations applicable to the entire investigation lifecycle rather than just the last-mile

VERSATILITY

Evolving Security Threats – *Handling the AI challenge*

Speed and Skill of attacks are vastly sophisticated

Using AI to gain knowledge of target(s) and launch personalized attacks for individual targets

AI Driven Malware adapting to environment

Malwares can be automated to obfuscate itself in order to bypass traditional detection techniques

Autonomous AI Powered Attacks with no Humans

Malicious actors leverage AI to launch a multi-faceted attack targeting infrastructure

What is the Customer Problem?

Alarm Overload

Customer NOC/SOC teams are unable to keep up with the large volume of alarms generated by the Versa platform and need a way to manage and triage them effectively.

Security Blind Spots

SOC teams lack visibility over their organization’s security posture, leading to complex threats going undetected. They need an easy way to manage, triage, and investigate alerts while integrating internal and external workflows.

Compliance Gaps

Security teams lack visibility over devices and assets that are out of compliance, and need a solution that not only surfaces these gaps but also automatically provides a path to resolving them.

What are the Adoption Enablers

Value

- **Cost** – Operational cost of implementing, incl. hidden licensing costs (storage, consumption, usage)
- **Resourcing** – Staffing to manage and review automations and outcomes incl. training
- **Compliance** – Compatibility with existing security investments for onboarding and consistent operation
- **Ease of Use** – Unified experience that enables adoption and analyst satisfaction

Features

- **Onboarding** – Off-the-shelf workflows and integrations that minimize configuration and setup
- **Case Management** – Pre-built tools to enhance investigations and streamline case handling
- **Customization** – Platform openness with ability to customize and integrate with other tools

Outcomes

- **Correlation** – Deliver visibility and context across security investments
- **Security** – Comprehensive use case detection & coverage
- **Operational** – Automated orchestration of security outcomes

Versa Behavioral Insights - *Vision*

Delivering unified AI-driven value across SecOps investigation, compliance, and threat management

Security Posture

Full visibility over attack surface vulnerability

- Attack Surface Management
- Shadow IT Discovery

Unified Experience

Single pane of glass for SOC and NOC alerts

- Centralized Investigation
- Reduced Alert Fatigue

SOC Acceleration

Faster investigations with automated remediation

- AI Threat Summaries
- Case Workflows
- GenAI via Verbo

Threat Management

Triage and respond to threats before escalation

- Real-time Updates
- Endpoint & 3rd-Party Detection

Lower TCO

Unified platform reducing operational costs

- Automated Risk Mitigation
- Integrated XDR

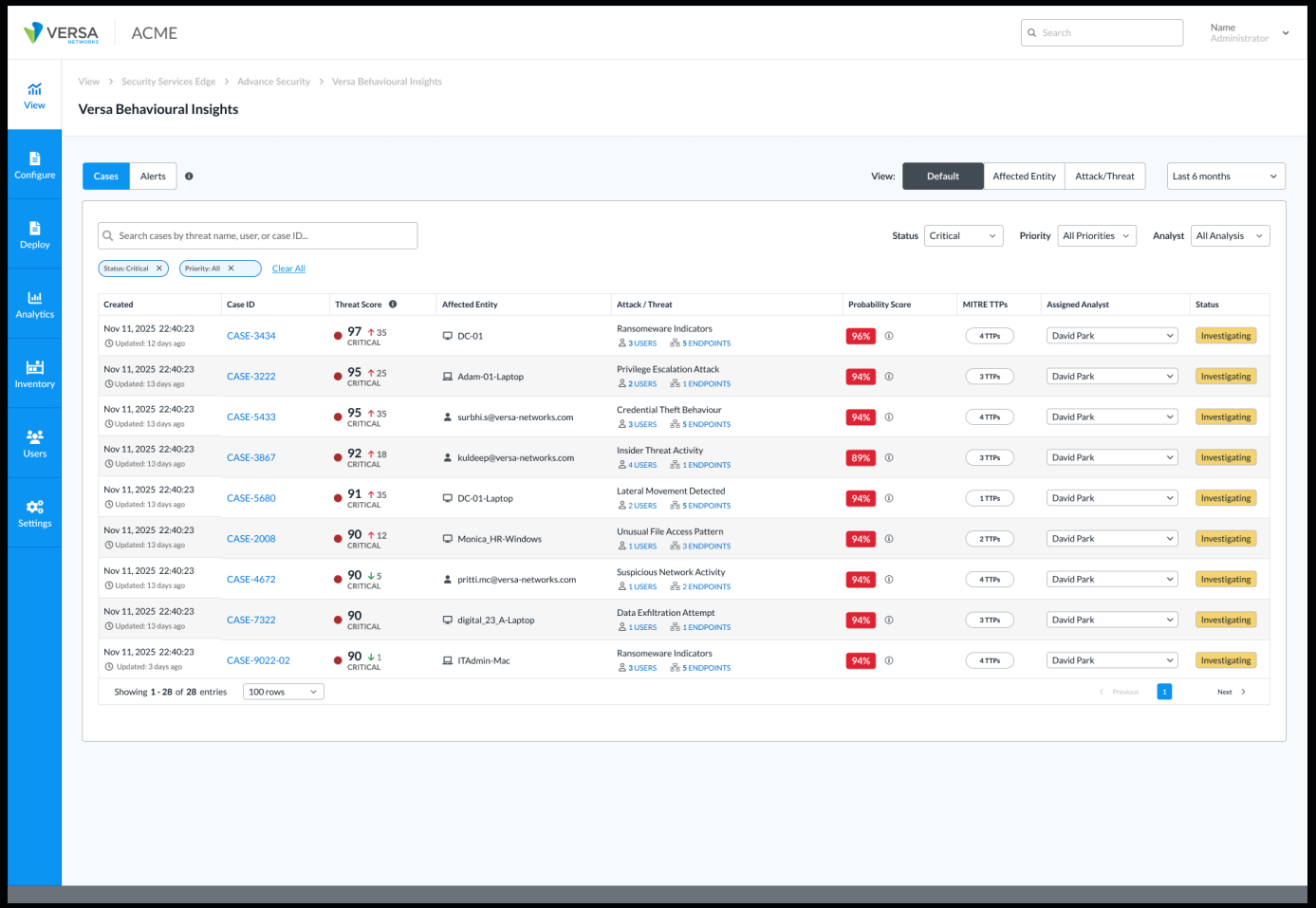
Agentic Orchestration

Intelligent, automated risk mitigation and orchestration

- AI-driven SecOps
- Automated Security enforcement

VERSATILITY

Versa Behavioral Insights - *AI insights for SecOps*



✓ Persona-based Centralized investigation experience

- **Actionable** Threat Insights – Reduce alert fatigue and noise
- Threat Management remediation incl. policy enforcement
- **Automated evidence** via Timelines for Threat Visibility

✓ Built-in investigation tools

- Real time threat updates incl automated **AI generated Threat Summaries**
- Attack Graph → Review blast surface
- Case Handoff and Approval workflows
- GenAI for SecOps via Verbo 2.x

✓ Live Updates

- Real-time updates as threats progress including evidence and **Risk profiles**

✓ Integrated Versa XDR capabilities

- **Enhanced Threat Insights** via Versa Endpoint agent
- Improved **Threat detection coverage** via 3rd party integrations

✓ Compliance coverage

- Vulnerability and **Attack Surface Management**
- **Shadow IT** and Non-user devices discovery and management

✓ Agentic SOC capabilities

- Intelligent, **automated Risk mitigation** and orchestration

VERSATILITY

Q&A