SUCCESS STORY

SNC establishes a robust, in-house security operations center with Elastic while scaling to ingest a tenfold increase in data

Region
United States

Industry
Public Sector

Solution
Elastic Security, SIEM, Microsoft Azure Government Cloud

Reduces query times from minutes to seconds

- With Elastic Security, SNC drastically reduced query times, increased analyst efficiency, and enabled its SOC to stay within internal and client-facing SLAs.

Ingests ten times the amount of security data

- With Elastic Security, SNC can scale to ingest a tenfold increase in data—the equivalent of a terabyte of data every day.

Enables launch of revenue-generating cloud security service

- SNC launched a cloud-based, managed security service via Elastic Security aimed at small and medium-sized defense contractors.

Leading aerospace and defense business deploys Elastic Security to protect their systems and launch cloud-based managed security services for other defense contractors

For SNC, a leading aerospace and national security contractor, robust cybersecurity is not just a best practice – it's a requirement. Stringent government regulations and the need to maintain client trust necessitate a comprehensive security posture across its spectrum of operations. This includes aircraft modification and integration, space components and systems development, and related technology products for cybersecurity and health design.

Elastic plays a pivotal role in this robust defense strategy, defending SNC against a range of threats, including cybercriminals, state-sponsored actors, and other malicious entities. Doug Russell, Director, Data Integration Strategies, SNC, emphasizes the significant improvement in performance compared to the previous SIEM solution managed by an external provider. "The legacy system was sluggish and expensive," he explains. "Running queries was a cumbersome process."

Russell's team opted to run Elastic concurrently with the existing solution to gain a firsthand perspective. The results were clear to see. "The difference was like night and day," Russell says. "Elastic's speed and querying capabilities within our environment blew us away. The ability to visualize data using Kibana dashboards was also impressive."

Taking control: building an in-house SOC

Driven by these results, SNC swiftly migrated to Elastic Security in full. This transition eliminated the need for an external managed service provider. "With Elastic Security as our central SIEM solution, we were able to establish a robust security operations center (SOC) entirely in-house," says Russell. This shift empowers SNC's cyber team to directly analyze and protect valuable intellectual property and Controlled Unclassified Information (CUI) without the help of a third party.

SNC delivers innovative, open architecture technology solutions that support and protect their customers, wherever their missions take them.

Another compelling advantage of Elastic lies in its robust automation capabilities. SNC has successfully automated a significant portion of its alerting workflows, enabling more efficient case tracking through Elastic's Case Management feature. "Elastic has helped us alleviate pressure on our security analysts while facilitating smoother data access," says Russell.

The team at SNC has also significantly benefited from Elastic's scalability. Elastic Security effortlessly manages a tenfold increase in data ingestion compared to the past solution—equivalent to a terabyte of data daily. This scalability empowers SNC to keep pace with the ever-expanding volume of security data generated in today's threat landscape.

Security speed and performance

Since deploying Elastic Security, SNC has dramatically improved query response times. "Results are now delivered in seconds or less, compared to the wait of several minutes with our previous SIEM," says Russell. "This enhanced speed is crucial for adhering to our strict SLAs with clients and ensures we remain within compliance boundaries."

Employees across the organization can now locate critical information in a fraction of the required time. This translates to efficiency gains in the highly competitive defense sector, where cost-effectiveness directly impacts government contract awards.

Elastic also excels in storage efficiency, addressing SNC's strict data retention requirements. Its ability to rapidly retrieve older data from cold and frozen storage tiers minimizes reliance on expensive hot access hardware. Features like searchable snapshots allow us to obtain swift answers from infrequently accessed data," says Russell.

Proactive threat detection and zero-day defense

SNC has achieved a crucial advantage in identifying and mitigating threats before they impact clients. "Elastic Security has empowered us to find, isolate, and neutralize zero-day attacks even before they're publicly announced," explains Russell. This proactive approach significantly strengthens SNC's security posture and minimizes potential damage.

> We can find threats quickly and alert clients before they have an inkling of what's going on in their environment. Other players in the defense sector haven't been able to keep up with us from a cybersecurity perspective."

Doug Russell
Director, Data Integration Strategies, SNC

Expanding business opportunities with managed security services

SNC saw a change in its fortunes when it offered its security operation as a cloud-based managed security service. "Elastic was a game-changer," states Russell. "We leveraged our experience to create a new revenue stream, fostering business growth and professional development for our security analysts."

Building on the combined strengths of Elastic Security and Microsoft Azure Government Cloud, the Defensible Security service empowers smaller and medium-sized defense contractors to safeguard their systems and comply with U.S. government regulations. This includes future regulations such as the Cybersecurity Maturity Model Certification (CMMC), which comes into effect in 2025.

"With Elastic and Microsoft, we extend protection beyond traditional IT systems, offering real-time defense for operational technology (OT) as well," explains Russell. "This comprehensive approach ensures comprehensive security coverage for client organizations."

Consolidation and streamlined operations

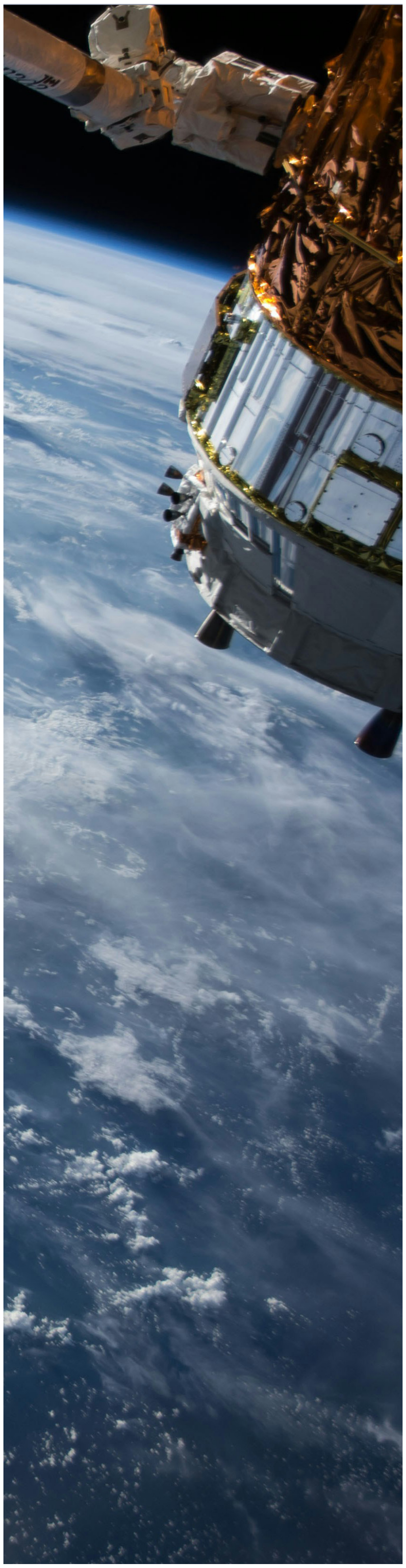
Elastic Security supports the consolidation of multiple security tools onto a single platform. Russell cites the example of identifying a malicious IP address. Previously, analysts would need to access multiple platforms for a complete picture. “The more tools involved, the more complex and expensive it becomes to maintain and operate the security infrastructure,” he explains. “Elastic elegantly addresses our requirements without unnecessary complexity or cost. It proved to be the most cost-effective solution, generating significant savings.”

Elastic Security fosters improved collaboration between SOC and incident response (IR) teams. Roderick Bickert, Cyber Security Manager, SNC, explains, “Previously, sharing information involved exchanging numerous links. With Elastic, we can send a single link that directs people to all available information, providing clear context for collaborators. Viewing everything within a unified platform significantly streamlines workflows.”

Exceptional support and continuous improvement

Beyond its solutions, Elastic provided invaluable consulting and support throughout the deployment. This proved particularly beneficial when SNC transitioned to offering managed security services. “Elastic’s support has been phenomenal,” says Russell. “They consistently go the extra mile to ensure our success.”

He values the ongoing guidance on optimizing existing and new features. “While we may not always have the time to test every new element, Elastic proactively ensures we maximize the value of our investment.”



AI/ML integration and advanced threat detection

SNC has ambitious plans to expand the use of AI and machine learning within its SOC. Elastic Security's data centralization capabilities are critical to this vision. Cassie Cagwin, Senior Cybersecurity Data Science Manager, SNC, says, "Regardless of data volume, we can store everything in a central location. This empowers us to apply any necessary logic, either within Elastic or by extracting data for external ML models. The results are then fed back to Elastic as alerts or rules."

She's particularly interested in leveraging Elastic's anomaly detection features. These capabilities automatically model normal time-series data behavior, enabling real-time anomaly identification, streamlined root cause analysis, and minimal false positives.

Another feature of significant interest is the out-of-the-box user entity behavior analytics (UEBA) tool. UEBA allows SNC to analyze not only user behavior but also the behavior of other entities within its systems, including devices and endpoints. "Elastic continues to play a central role in our AI security initiatives," says Cagwin.

> Elastic Security has been instrumental in transforming our security posture. Its scalability and powerful search capabilities are ideal for the aerospace and defense sector, enabling us to detect and respond to threats faster and more effectively."

Doug Russell
Director, Data Integration Strategies, SNC

Schedule a 1:1 session with an Elastic expert who can help you land on the right approach and architecture for your organization's IT strategy and mission goals.

Get in touch