ThreatConnect.

Customer Spotlight

Genuine Parts Company Modernizes Cyber Risk Management with ThreatConnect

Customer Profile

Organization size
60,000 EMPLOYEES
10,700 LOCATIONS
17 COUNTRIES

Industry / Sector
AUTOMOTIVE & INDUSTRIAL SUPPLIES

Headquarters
ATLANTA, GA

Background

Genuine Parts Company (GPC) is a world-class distribution organization involved in automotive and industrial replacement parts operating two primary lines of business over almost 11,000 locations across 17 countries. GPC required a robust solution to quantify and effectively manage the cyber risks of critical business assets. CGS CyberDefense partnered with ThreatConnect to implement Risk Quantifier (RQ) for GPC to enable the financial quantification of cyber risks in order to improve risk communications, optimize GPC's security investments, and prioritize their cybersecurity initiatives.

Challenges Faced

GPC faced several common challenges in improving their cyber risk management program.
For example:

- Prioritizing risks and investments associated with new business critical applications and existing assets (applications and data).
- Security and business leaders struggled to understand which projects offered the best ROI
- Ensuring cyber risk is adequately communicated to and understood by leadership and the board when defining and allocating cybersecurity investments

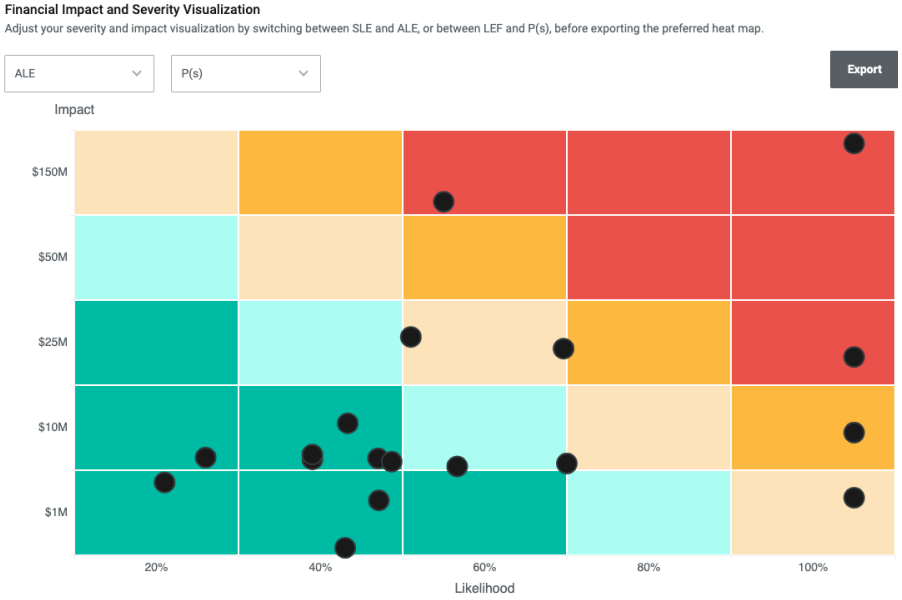
How ThreatConnect Helped

ThreatConnect RQ enabled GPC to move from qualitative to quantitative risk posture for their business critical assets with little friction. For example, GPC was able to quantify the max single loss event (SLE) and annual loss exposure (ALE), as well as the probability of a successful cyber threat event for a business critical application with millions of PII records. RQ was also able to provide granular details on where losses would be realized, e.g., lawsuit settlement, remediation costs, and legal fees.

> "ThreatConnect has significantly enhanced our decision-making process. By incorporating risk metrics like the Single Loss Exposure and Annual Loss Exposure, we can now fully evaluate and prioritize remediation efforts more effectively, beyond just cost and effort considerations. This has led us to reassess previous decisions to ensure we're addressing the highest risks. Additionally, the ability to track risk reduction allows us to clearly demonstrate the ROI of our security initiatives."
>
> **Damian A. Apone, Global Director - Governance, Risk, & Compliance**
>
> **Enterprise Security I Genuine Parts Company**

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240



An example heatmap representation of how CRQ displays the correlation of financial impact and the likelihood of various cyber risk events (represented by dots).

Note: this dataset is not using real data

~41 Million

PII Records at Risk

$31 M Max Loss (SLE)

& $5M Annual Loss (ALE)

45% Probability

of a successful threat event

Additionally, as GPC has expanded their CRQ program, they have begun to utilize additional capabilities within ThreatConnect RQ, like integrating vulnerability scan data. This allows GPC to have a better understanding of which vulnerabilities are critical to them in terms of dollars and cents rather than relying on a CVE score.

Lastly, GPC has begun to incorporate CRQ into their third-party risk management process. With ThreatConnect's integration with Security ScoreCard, GPC has been able to look at critical vendors from a more data-driven point of view rather than the typical qualitative – critical, high, medium, low – risk commonly used across enterprises today.

By employing ThreatConnect RQ, GPC can now prioritize security initiatives based on the financial impact of risks, ensuring budgets are allocated to projects offering the most significant reduction in financial risk. Ultimately, ThreatConnect empowered GPC to measure and communicate cyber risk, prioritize responses, justify budgets and spend allocation, and make better informed investment decisions to manage their cybersecurity effectively.

In Conclusion

The implementation of ThreatConnect RQ was transformative for GPC, improving clarity in cyber risk communications and prioritization for its cybersecurity strategy and investments. GPC can now confidently justify security investments, prioritize its response efforts, and optimize its budget allocation based on a clear understanding of financial risk. With the expertise of CGS CyberDefense and the powerful capabilities of ThreatConnect RQ, GPC achieved a more resilient and financially sound cybersecurity posture, ensuring the protection of its critical assets and business operations.

About ThreatConnect:

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240