Evaluation of the GRIT 2025 Ransomware & Cyber Threat Report

Structural, Analytical, and Functional Deficiencies – GUIDEPOINT SECURITY

https://www.guidepointsecurity.com/resources/grit-2025-ransomware-and-cyber-threat-report/

Are assessment is an unsolicited view of an organization's public-facing report. We assess reports of these types in our training classes as examples we breakdown and analyze against analytic standards. The following is such an assessment.

The GRIT 2025 Ransomware & Cyber Threat Report presents a comprehensive effort to document the evolving dynamics of ransomware activity and cybercrime. While the report provides substantial data and insights into threat actor behavior, its effectiveness as an intelligence product is limited by significant gaps in analytic rigor, structural clarity, and source reliability. Decision-makers rely on precise, actionable intelligence to address emerging threats, yet the report struggles to meet those expectations due to its lack of methodological depth and misaligned priorities. A thorough analysis of its strengths and weaknesses reveals the improvements necessary to transform it into a reliable resource for informed decision-making. Addressing those deficiencies will enhance the report's ability to guide stakeholders through the complexities of cyber threat intelligence. However, key deficiencies in structural standards affect its accessibility.

Detailed Assessment of the GRIT 2025 Ransomware & Cyber Threat Report

We critically evaluated the GRIT 2025 Ransomware & Cyber Threat Report based on strict intelligence writing standards (CIA, DIA, DNI), structured analytic techniques (SATs), and critical thinking frameworks. The evaluation includes detailed analysis, examples, and actionable recommendations.

The GRIT report shows some organizational strengths but is hindered by structural flaws that undermine its accessibility and impact. The report does not present key findings, implications, or actionable recommendations at the outset and violates intelligence writing standards, leaving readers without a clear understanding of the report's relevance. For instance, the "Note from GRIT" emphasizes collaboration with incident response teams but

lacks a concise summary of its primary conclusions. Presenting actionable insights upfront, such as specific ransomware group impacts or trends, enhances clarity and engagement.

The Methodology section is another area where structural inefficiencies detract from the report's value. Repeated disclaimers about source variability and reliability, while necessary, become redundant and overly generalized. Instead of quantifying the implications of these issues, the section leaves readers guessing about the extent to which data reliability affects the analysis, including specific metrics, such as estimating the percentage of data affected by threat actor denial tactics, improving transparency, and contextualizing the limitations.

In terms of analytic rigor, the report falls short of professional intelligence standards. Foundational structured analytic techniques, such as the Analysis of Competing Hypotheses (ACH) and Key Assumptions Check, are notably absent. The omission weakens the ability to explore alternative explanations for observed trends. For example, the report attributes a decline in ransomware activity solely to law enforcement crackdowns but does not consider other plausible factors, such as enhanced corporate defenses or changes in economic conditions. Applying ACH allows for a more balanced exploration of such possibilities, reducing the risk of confirmation bias and strengthening the overall analysis.

The report also lacks diagnostic depth, often presenting general conclusions without differentiating between diagnostic and non-diagnostic evidence. For instance, it mentions that "Developing ransomware groups recruit experienced operators" but does not explore how this behavior sets them apart from Splinter groups. Analyzing comparative success rates or attack patterns provides the diagnostic evidence needed to substantiate such claims and deepen the reader's understanding of group dynamics.

Accuracy and evidence quality further weaken the report's impact. Heavy reliance on threat actor blogs and unverified victim claims introduces significant risks of inaccuracy. Statements such as "Ransomware Group Y claims to have breached 500 organizations" are presented without independent verification or corroboration through law enforcement data or leaked samples. The tendency to favor single narratives, such as attributing ransomware group rebranding solely to law enforcement pressure, overlooks other potential drivers like financial incentives or internal disputes. Greater emphasis on evidence triangulation and alternative explanations addresses these shortcomings.

Functionally, the report does not translate its analysis into actionable intelligence for stakeholders. The report identifies trends, such as increasing encryption sophistication, without offering prioritized recommendations or clear mitigation strategies. For example, it mentions trends but neglects to recommend specific actions, such as deploying advanced decryption tools or enhancing endpoint detection capabilities. The absence of scenario

planning further reduces its strategic utility. Techniques like Alternative Futures Analysis project how ransomware trends evolve, offering decision-makers foresight into emerging threats and adaptive strategies.

The report misses valuable opportunities to enrich its analysis through case studies and geospatial data. While it mentions "Ephemeral" ransomware groups, it does not give concrete examples to contextualize their behavior. Including a detailed case study of a short-lived group clarify their operational characteristics. Similarly, geospatial tools map ransomware activity by region, creating visual representations that convey complex data more effectively and enhance stakeholder understanding.

In its current state, the report remains a descriptive product that struggles to align its findings with actionable outcomes. Addressing its structural flaws, improving analytical depth, and incorporating practical recommendations transform it into a more reliable and impactful intelligence resource.

The GRIT 2025 report shows effort but fails to meet professional intelligence standards in structure, analysis, and actionable insight. The report evolves into a more impactful and reliable intelligence product by addressing structural flaws, improving analytic rigor, and providing targeted recommendations,

Excessive Use of Jargon

The report uses technical and overly detailed language without sufficient explanation for a broader audience. The report alienates stakeholders with varying levels of technical proficiency. The GRIT 2025 Ransomware & Cyber Threat Report exhibits an excessive reliance on technical jargon and detailed language that lacks sufficient context or explanation for a non-specialized audience. The issue is evident throughout the document and creates barriers to understanding, particularly for stakeholders who may not possess extensive technical expertise in cyber threats or ransomware operations.

For instance, the report uses terms like "Splinter," "Rebrand," and "Ephemeral" to categorize ransomware groups. While these classifications are helpful for internal analysis, they are not defined in a way that a broader audience can easily grasp. The explanation provided for "Splinter groups," for example, mentions that they consist of members from previously established groups and retain overlapping tactics, techniques, and procedures (TTPs). However, the report does not illustrate this with practical examples or analogies. A hypothetical or real-world case study clarifies how these dynamics manifest in practice. An example is a well-documented ransomware group that fragmented due to leadership disputes or operational failures,

Similarly, the term "Ephemeral" is defined as referring to short-lived groups with low victim counts, often operating for less than three months. However, the explanation remains abstract without concrete data or examples to illustrate what makes these groups distinct from others. For readers unfamiliar with cybercriminal behavior, this lack of tangible reference diminishes the impact and accessibility of the analysis.

Another example of excessive jargon appears in the methodology section, where phrases like "denial and deception tactics" and "refined from relevant tactical details" are used without elaborating on their specific meaning in the ransomware context. While these terms may be common in intelligence circles, they are not intuitive for broader audiences, including corporate leaders or policymakers who may rely on this report to inform decisions. Providing a brief explanation of denial and deception tactics, such as threat actors fabricating attack claims to sow confusion among analysts, makes the content more digestible.

The taxonomy of ransomware groups also uses phrases like "operational maturity and sophistication" to describe group behaviors. However, no benchmarks or criteria are provided to quantify or qualify what constitutes "maturity" or "sophistication." For example, saying that a group has "achieved operational maturity by conducting more than 50 successful attacks within six months" offers a clearer insight into how these terms are applied. Instead, the lack of clarity risks alienating readers unfamiliar with industry-specific terminology.

The cumulative effect of such jargon and detailed language without sufficient explanation undermines the report's accessibility. Stakeholders with varying levels of technical knowledge, from business executives to policymakers, may find it challenging to extract actionable insights from the document. The report should adopt a more reader-friendly approach by integrating plain language, context-driven examples, and analogies that bridge the gap between technical content and practical understanding.

Overreliance on Raw Data

Methodological explanations are repetitive and convoluted, detracting from actionable insights. Summaries of trends and implications should be concise and immediately informative.

The GRIT 2025 report demonstrates a significant overreliance on presenting raw data, accompanied by methodological explanations that are repetitive, convoluted, and ultimately detract from the delivery of actionable insights. While the intention to provide transparency regarding the methodology is commendable, the report devotes excessive

space to outlining its approach without translating the findings into clear, concise summaries that address the implications of the trends it uncovers.

For example, in the methodology section, the report repeatedly emphasizes the variability and unreliability of data sourced from ransomware threat blogs. It acknowledges the inherent challenges of verifying claims made by these groups, such as inflated attack numbers or exaggerated financial demands. However, the text revisits this point multiple times, using similar phrasing, without advancing the discussion or providing actionable alternatives. Readers are left with the impression that the report is overly focused on justifying its process rather than presenting meaningful insights drawn from the available data. This repetition reduces the overall clarity and utility of the methodology section, which instead has been streamlined into a single, well-organized explanation.

The report also dedicates extensive text to quantifying observed attack trends, such as the frequency of victim postings or the operational timelines of specific ransomware groups. While raw figures like "Group X posted 20 victims in one month" are useful, they are presented without sufficient context or interpretation to guide decision-making. For instance, the report fails to answer critical follow-up questions: How is this trend compared to previous years? What industries or regions were disproportionately affected? What are the strategic implications for organizations within the targeted sectors? Raw data becomes a missed opportunity to provide deeper, actionable intelligence by leaving these questions unanswered.

Another issue is the presentation of raw numbers without synthesis. For example, the report highlights the decline in victim counts for certain ransomware groups but does not adequately explore the factors driving this decline. Whether it stems from increased law enforcement pressure, improved defensive measures by organizations, or internal fragmentation within the threat groups is still unexplored. Readers must draw their conclusions from a sea of data points rather than be guided through a well-reasoned analysis that connects the dots and draws out key implications.

The section on trends further illustrates the overreliance on raw data. While it enumerates various shifts, such as the rise of "extortion-only" groups, it spends more time quantifying the phenomenon than analyzing its broader impact. For instance, the report notes that extortion-only groups are becoming more prevalent but does not explore the strategic risks this poses for organizations that focus exclusively on ransomware defense. A concise synthesis of this trend, coupled with recommendations for mitigation strategies, has been far more valuable than the overly detailed descriptions of individual data points.

This reliance on raw data, combined with repetitive and overly detailed methodological explanations, hinders the report's effectiveness as a tool for decision-making. Decision-makers, particularly those in leadership positions or with limited technical backgrounds, require clear and concise summaries of trends, implications, and recommended actions. The absence of such clarity reduces the practical value of the report, leaving readers overwhelmed with information but underserved in actionable guidance.

Competency in Analysis

Despite substantial effort in data collection, analytical rigor is inconsistent-

- Application of Structured Analytic Techniques- Techniques such as the Key Assumptions Check, Indicators Validator, and Alternative Futures Analysis are underutilized. The report does not clearly challenge its assumptions or present alternative scenarios.
- Gaps in Diagnosticity- The analysis often supports preconceived narratives rather than exploring competing hypotheses, which reduces its credibility and robustness.
- Methodology Transparency- While the methodology section outlines data sources, it lacks explicit discussion of source evaluation, reliability, and potential biases.

The GRIT 2025 report demonstrates inconsistency in its analytical rigor despite evident effort in data collection. While it attempts to address complex ransomware and cyber threat trends, the absence of robust application of structured analytic techniques, a lack of diagnostic analysis, and limited methodological transparency hinder its credibility and overall effectiveness.

The report fails to adequately incorporate structured analytic techniques (SATs) that are critical for challenging assumptions, exploring alternative explanations, and addressing uncertainty. Techniques such as the Key Assumptions Check, Indicators Validator, and Alternative Futures Analysis, which are standard practices in professional intelligence analysis, appear largely absent. For example, the report discusses shifts in ransomware group tactics but does not explicitly examine the underlying assumptions driving these trends. It attributes increased rebranding among ransomware groups solely to efforts to avoid law enforcement detection, but it neglects to explore other plausible scenarios, such as internal group conflict, changes in financial motivation, or competitive pressures among criminal actors. Without applying an Alternative Futures Analysis to project potential trajectories of ransomware operations, the analysis remains limited to a single narrative, leaving decision-makers unprepared for unexpected developments.

The report further exhibits gaps in diagnosticity, as much of the analysis supports preconceived conclusions rather than thoroughly testing alternative hypotheses. For instance, the section on emerging ransomware trends highlights the rise of extortion-only groups, attributing this shift to reduced operational risk. However, it does not consider other possibilities, such as technological constraints preventing encryption-based attacks or broader economic pressures forcing groups to adopt leaner operations. By failing to identify evidence that refutes the dominant narrative, the report diminishes its robustness and opens itself to the influence of confirmation bias. A more balanced approach, such as examining how this trend aligns or conflicts with industry-wide threat intelligence, has enhanced the analysis and improved its credibility.

The methodology section, while providing an overview of data collection practices, lacks transparency regarding the evaluation of source reliability and potential biases. The report acknowledges the inherent challenges of relying on threat actor blogs and public victim disclosures but stops short of explaining how these sources were vetted or how biases were mitigated. For example, it states that certain threat actor claims were excluded due to apparent fabrication but does not detail the criteria used to make such determinations. Additionally, the report does not clarify whether independent corroboration, such as cross-referencing claims with law enforcement reports or open-source intelligence, was conducted to validate its findings. This absence of explicit discussion leaves readers uncertain about the rigor of the data and undermines confidence in the report's conclusions.

Overall, while the GRIT 2025 report provides a substantial dataset and attempts to analyze ransomware and cybercrime trends, its inconsistent application of structured analytic techniques, reliance on narratives lacking diagnostic balance, and limited methodological transparency significantly diminish its analytical strength. These shortcomings reduce their value as a tool for stakeholders who rely on objective, rigorous analysis to inform decision-making and prepare for emerging threats.

Accuracy and Evidence

The report attempts to quantify trends but struggles with ensuring accuracy-

- Source Reliability and Validation- The heavy reliance on threat group blogs and unverified victim claims introduces potential inaccuracies. While the report acknowledges this, it does not adequately mitigate these risks by triangulating data or employing alternative evidence sources.

- Bias in Interpretation- Certain conclusions, such as threat actor motivations and effectiveness of countermeasures, lack robust evidence. There is a tendency toward confirmatory bias rather than presenting a balanced assessment.

The GRIT 2025 report endeavors to quantify trends within the ransomware and cybercrime landscape, but it faces considerable challenges in ensuring the accuracy of its findings. These issues stem from a reliance on unverified data sources and interpretative biases that weaken the validity and credibility of its conclusions.

The report heavily depends on threat group blogs and victim claims as primary data sources. While it acknowledges the inherent risks associated with these sources, including exaggeration and denial tactics by threat actors, it does little to mitigate the inaccuracies that arise. For instance, claims by ransomware groups regarding the number of their victims or the financial value of their attacks are presented as data points without sufficient corroboration. The report does not indicate that it attempted to triangulate these claims with independent evidence, such as law enforcement data, victim-reported incidents, or third-party cybersecurity analyses. This lack of source validation leaves readers uncertain about whether the data presented is an accurate reflection of the threat environment or merely a reflection of the group's propaganda efforts. Without the application of systematic validation methods, such as cross-referencing victim claims with known attack patterns or verifying financial data against blockchain analysis tools, the reliability of the report's findings is compromised.

Beyond source reliability, the report exhibits bias in its interpretation of trends and threat actor behavior. Its conclusions regarding ransomware group motivations and the effectiveness of countermeasures often lack a balanced assessment supported by robust evidence. For example, the report asserts that law enforcement crackdowns have significantly curtailed the activity of established ransomware groups. However, it provides no comparative analysis or statistical evidence to substantiate this claim. Other plausible explanations, such as improved organizational defenses or internal shifts within criminal networks, are not explored. This tendency to favor a single explanatory narrative reflects a form of confirmatory bias, where evidence is interpreted in a way that supports pre-existing assumptions rather than rigorously challenging them. The failure to present alternative explanations diminishes the analytical objectivity of the report, leaving its conclusions vulnerable to critique.

The absence of a transparent approach to managing these issues further exacerbates concerns over the report's accuracy. Without explicitly detailing how sources were evaluated for reliability or explaining the methodology for interpreting key trends, the analysis risks

appear superficial or incomplete. This lack of rigor undermines the report's ability to provide actionable intelligence and creates potential blind spots in understanding the evolving cyber threat landscape. By failing to address these issues, the GRIT 2025 report ultimately struggles to establish itself as a reliable and authoritative resource for stakeholders seeking to navigate the complexities of ransomware and cybercrime.

Functional Impact

The report provides a broad overview but struggles to convert its analysis into actionable intelligence-

- Policy-Relevant Intelligence- The report fails to align its findings with specific policymaker or organizational needs, a fundamental requirement in Sherman Kent's analytic doctrine.
- Decision-Making Utility- The absence of prioritized recommendations or risk-based assessments reduces its usability for strategic decision-making.

The GRIT 2025 report offers a broad overview of ransomware and cybercrime trends but falls short in transforming its analysis into actionable intelligence. This limitation is particularly evident in its inability to address the needs of policymakers and organizations and in its failure to provide practical guidance for decision-making. These shortcomings severely undermine its functional impact, reducing its value as a strategic resource.

The report does not effectively align its findings with the specific requirements of policymakers or organizational stakeholders, a core principle of Sherman Kent's analytic doctrine. According to Kent, intelligence analysis must prioritize relevance to decision-makers, ensuring it directly supports their operational, tactical, or strategic objectives. The GRIT 2025 report, however, lacks the focused tailoring necessary to meet these needs. For instance, while the report discusses the rise of "extortion-only" ransomware groups, it does not offer insights into how this trend influences policymaker decisions related to resource allocation, law enforcement strategies, or legislative frameworks. Similarly, organizational leaders seeking to protect critical infrastructure find little guidance on specific defensive actions to mitigate these emerging threats. The report misses the opportunity to bridge the gap between analysis and policymaker or organizational priorities.

In addition to its lack of policy relevance, the report struggles to provide decision-making utility due to the absence of prioritized recommendations or risk-based assessments. While the document identifies trends and behaviors within the ransomware ecosystem, it fails to articulate actionable steps that stakeholders should take in response. For example, the report identifies ransomware groups transitioning to more targeted attacks but does not

prioritize which sectors or geographies are at the greatest risk. Without a hierarchy of risks or actionable recommendations, such as investing in specific technologies or focusing on vulnerabilities, decision-makers are left without a clear roadmap for addressing the threats identified. Furthermore, the report does not quantify potential risks or impacts, such as the financial or operational consequences of emerging ransomware tactics, leaving stakeholders unable to evaluate the urgency or severity of these threats effectively.

The absence of actionable intelligence limits the report's practical value and undermines its ability to inform strategic planning. Stakeholders rely on intelligence products to guide resource allocation, establish priorities, and anticipate adversarial moves. Without actionable insights or a clear connection to decision-making processes, the GRIT 2025 report remains a descriptive document rather than a prescriptive tool. The report must shift from broad overviews to targeted analyses that directly support the objectives of its audience, providing the practical guidance necessary for informed, effective decision-making.

Recommendations for Improvement

- Reorganize to Adopt Intelligence Writing Standards- Implement analytic brief structure for all major sections, ensuring clarity and accessibility for diverse audiences.
- Enhance Analytic Rigor
    - Use the Analysis of Competing Hypotheses (ACH) to explore alternative scenarios and mitigate cognitive biases.
    - Conduct a Key Assumptions Check to identify and validate underlying premises.
- Improve Source Reliability
    - Evaluate sources using frameworks such as the CRAAP test, explicitly scoring for relevance, accuracy, and authority.
    - Diversify data inputs to include verifiable and independent sources, such as law enforcement or cybersecurity research.
- Translate Data into Actionable Insights- Develop concise, prioritized recommendations with clear implications for stakeholders. Include scenario planning to prepare for future contingencies.

- Enhance Visual Presentation- Use geospatial and trend analysis tools for dynamic visualizations that convey trends and risks effectively.

The GRIT 2025 report requires significant improvements to increase its value and effectiveness as an intelligence product. Addressing its structural, analytical, and presentational shortcomings will address professional intelligence standards and enhance its usability for diverse audiences, including policymakers, organizational leaders, and other stakeholders.

The report should be reorganized to adopt intelligence writing standards, with a specific focus on implementing analytic writing structure and format. The reorganized report positions key findings, implications, and recommendations at the beginning of each section, ensuring immediate clarity and accessibility. The report better engages readers and provides them with a clear understanding of its relevance before delving into supporting details by presenting the most critical information upfront. For instance, sections discussing ransomware trends begin with an executive summary showing the most impactful trends, such as the rise of "extortion-only" groups, followed by an outline of their implications for targeted industries.

Enhancing analytic rigor is another essential step for improvement. Incorporating structured analytic techniques, such as the Analysis of Competing Hypotheses (ACH), enables the report to explore alternative scenarios and address potential cognitive biases systematically. For example, instead of attributing changes in ransomware activity solely to law enforcement crackdowns, ACH allows the report to consider other explanations, such as economic pressures or internal group dynamics. Conducting a Key Assumptions Check further strengthens the analysis by finding and confirming the premises underlying its conclusions. This process helps find flawed assumptions, such as overestimating the operational capacity of specific ransomware groups, and refine the overall narrative.

Source reliability must be addressed more rigorously to enhance the credibility of the report. Using frameworks like the CRAAP test helps score data for relevance, accuracy, and authority. The current reliance on threat actor blogs and unverified victim claims introduces risks that are mitigated by incorporating verifiable and independent data sources, such as law enforcement reports, cybersecurity firm analyses, or blockchain transaction audits. This diversification improves the reliability of the data and provides a more balanced foundation for the report's conclusions.

The report must also prioritize translating data into actionable insights. Developing concise, prioritized recommendations that highlight clear implications for stakeholders increases the utility of the analysis. For instance, showing the sectors most vulnerable to "extortion-only"

attacks and recommending specific defensive measures bridge the gap between analysis and implementation. Scenario planning, like potential ransomware evolutions under varying enforcement or economic conditions, prepares stakeholders for future contingencies.

Finally, the visual presentation of the report should convey trends and risks effectively. Using geospatial tools and dynamic visualizations, such as heatmaps, illustrating regional attack frequency or trend charts to track the rise of specific ransomware tactics makes the findings more accessible and engaging. Visual aids simplify complex data, allowing readers to grasp key points quickly and facilitating better strategic decision-making.

Implementing these changes will transform the GRIT 2025 report from a descriptive analysis into a prescriptive and impactful intelligence product. By addressing structural, analytical, and presentation weaknesses, the report will better serve its intended purpose of guiding decision-makers through the complexities of the ransomware and cybercrime landscape.

The GRIT 2025 report reflects a commendable level of effort in the collection of cyber threat intelligence, but it falls short in critical areas that undermine its effectiveness. Significant improvements in analytic rigor, structural organization, and source validation are essential to elevate the report to professional intelligence standards. These deficiencies hinder the report's ability to provide actionable insights, diminish its credibility, and limit its value as a resource for decision-makers.

Analytic rigor is notably lacking throughout the report, as it does not incorporate essential structured analytic techniques or challenge its assumptions effectively. The analysis remains descriptive rather than prescriptive, offering a limited exploration of alternative explanations for observed trends. Without addressing competing hypotheses or conducting robust evaluations of evidence, the report risks presenting a skewed or incomplete understanding of the cybercrime landscape. Decision-makers rely on intelligence products to make informed, strategic decisions, and the absence of rigorous analytic processes diminishes the reliability of the insights provided.

Structural organization further detracts from the report's utility. The lack of adherence to intelligence writing standards complicates comprehension and delays access to the report's core findings. Instead of presenting key conclusions upfront, the analysis becomes mired in excessive detail and methodological explanations, leaving readers to sift through unnecessary information to discern actionable takeaways. A more concise and organized approach streamlines the content, enhances accessibility, and better caters to the needs of its intended audience.

The report also suffers from insufficient source validation, relying heavily on unverified claims from threat actors and victim disclosures without adequate corroboration. This reliance introduces significant risks of inaccuracies and undermines confidence in the findings. Failure to cross-reference data with independent and reliable sources, such as law enforcement records or blockchain analysis tools, further compounds this issue. Decision-makers require intelligence products grounded in verified data to trust the recommendations presented, and the current approach does not meet that standard.

Addressing these issues will significantly enhance the report's credibility and utility. Improvements in analytic rigor will provide a more balanced and robust analysis, while better structural organization will make the content more accessible and actionable for stakeholders. Strengthening source validation will ensure the reliability of the findings, fostering greater confidence in the report's conclusions. The GRIT 2025 report can evolve into a professional-grade intelligence product capable of meeting the needs of decision-makers navigating the complex landscape of cyber threats.

