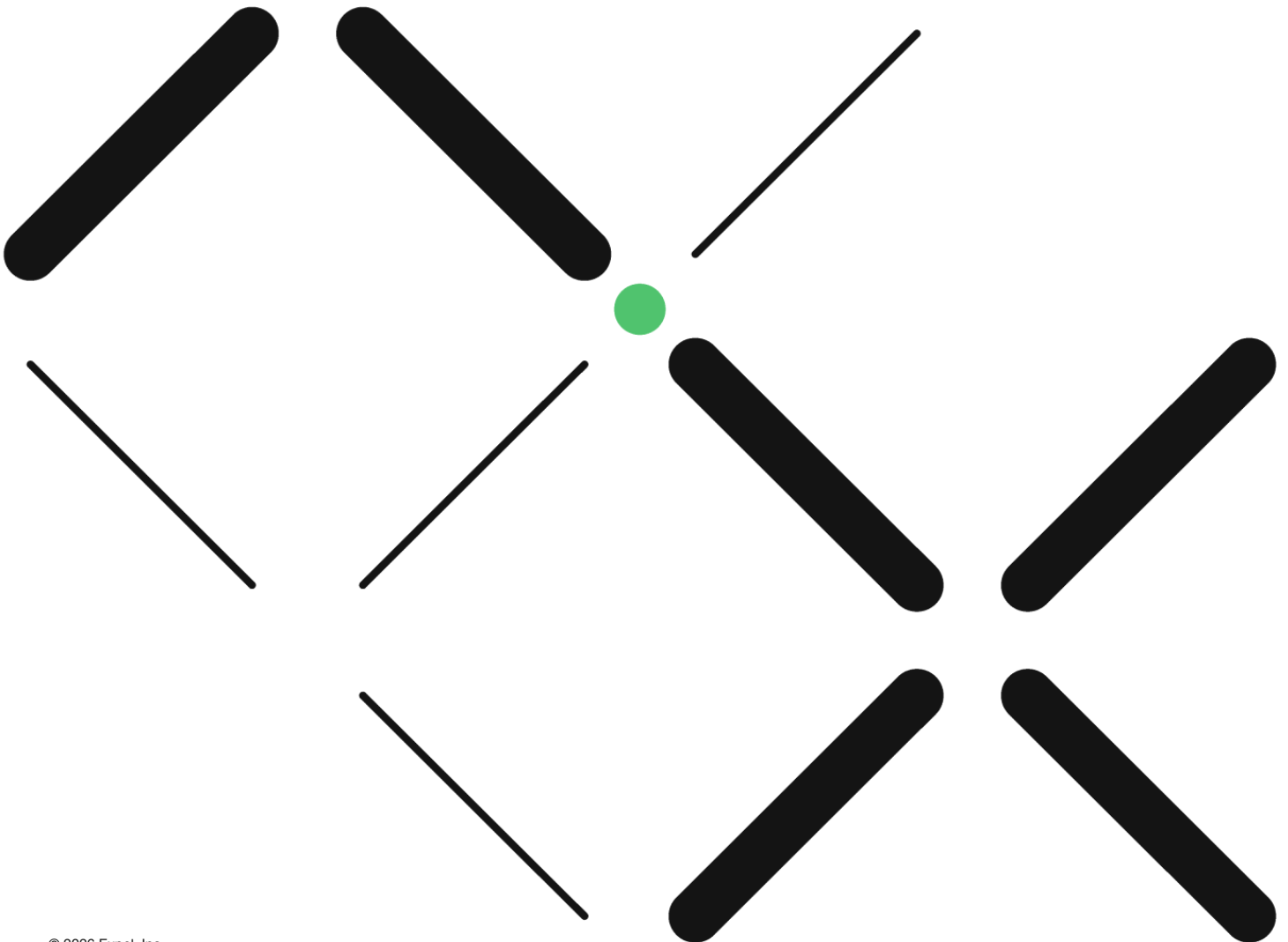




Introducing the SOC Metrics & Efficiency KPIs Dashboard Tool

Brought to you by the team at Expel

April, 2026



Why we built this tool

Your security operations center (SOC) is your front line, but are you truly measuring its impact? You need data to know for sure—after all, security without metrics is just wishful thinking.

We built this tool to help you track what matters, from team performance to ROI. You'll get clear, actionable metrics based on our expertise and experience protecting major organizations worldwide.

And since nearly half of security teams want better SOC metrics (according to SANS research), you'll be ahead of the curve with comprehensive data to prove your security investments are paying off.

NOTE: This is NOT an exhaustive list of all SOC metrics and KPIs to track. In fact, there are many more metrics that we internally track at Expel, and more that you most likely would want to track outside of this tool. We suggest you use this tool as a starting place, and add to it as your security operations evolve. We encourage you to measure any and all metrics that you feel are appropriate to track for your business.

Ready to get started?

Stop guessing, start knowing. Dive into this SOC Metrics & Efficiency KPIs Dashboard Tool today, and take the first step towards a data-driven, high-performing SOC. And when you're ready to truly transform your security posture, remember—Expel is here to help you level up.

How to use the dashboard

Step 1: Enter your foundational info and this month's metrics

Time to start building your dashboard! Complete this first, and you'll see the key metrics populate in the "SOC KPIs Dashboard" tab.

1. Navigate to the "This Month's Inputs" tab.
2. Fill in your security program's essential details. Editable cells are shaded yellow. Just looking for critical info here, things like:

- SOC team: your people power
- Alert management: the daily grind, quantified
- Incident response: speed kills (threats, that is.)
- Operational-level agreements (OLA): your internal targets
- Detection engineering: proactive defense is key

Why is this important?

The data you enter in this "Inputs" tab shapes everything—from understanding your current performance, to planning for growth. Get this wrong, and the whole analysis won't be useful. Take your time getting these numbers right, and you'll have solid proof of your security team's impact. So, don't just fill in boxes—build a data-driven foundation for SOC success.

Step 2: Add monthly data to analyze your trends over time

Consistent, monthly tracking is the lifeblood of this tool. Don't just set it and forget it—commit to monthly data entry. This is where you uncover the real story of your SOC's performance.

1. Navigate to the "Monthly Tracking" tab.
2. Select your starting month and year: The tool will adjust to reflect the month and year you select.
3. Enter your key performance data, month by month: Copy the data you entered on the "This Month's Inputs" tab into the appropriate month in the table in the "Monthly Tracking" tab to analyze your metrics month-over-month, comparing up to 24 months of data.

Why is this important?

Looking at your SOC data month-to-month reveals the real story. By monitoring these trends continuously, you'll spot critical changes in workload, efficiency gains, or losses, incident response improvements or slowdowns, and how well your detection systems perform over time. This isn't just about creating reports. It's turning your metrics into actionable insights that drive continuous improvement.

Step 3: Unlock the insights

This is the payoff. The "SOC KPIs Dashboard" tab is where your data comes to life. Here's the real picture of your SOC's efficiency and the key metrics to track.

1. Navigate to the "SOC KPIs Dashboard" tab.
2. Review your key performance indicators (KPIs) at a glance: The dashboard automatically visualizes your data, presenting your KPIs in clear, digestible charts and graphs. You can select the tabs at the top to jump down the page to that section.
3. Identify trends and patterns: If you input your monthly metrics, you can start to see trends. Is workload increasing month over month? Is efficiency improving? Is incident response time decreasing? The dashboard visually highlights any patterns.

Why is this important?

Visualizations make data understandable and actionable. The dashboard provides a clear, concise view of your SOC's performance. No more drowning in data or trying to understand where the bottlenecks are—just clear, actionable insights.

Step 4: Share your metrics internally

Data is powerful, but only if you can communicate it effectively. The "Printable KPI Scorecard" is your one-page secret weapon for demonstrating your SOC's performance to leadership and stakeholders.

1. Navigate to the "Printable KPI Scorecard" tab.
2. Review your executive summary: This tab automatically generates a concise, one-page summary of your key SOC metrics to share with leadership.
3. Print or export for easy sharing: Easily print or export this page as a PDF and share it with your manager, your CISO—anyone who needs to understand the ROI of your SOC investments. We suggest setting your print settings to: Print: "Active Sheets", Margin: "Narrow Margins", Orientation: "Portrait", and select checkbox: "Scale to fit: 1 page wide by 1 pages tall".

Why is this important?

Leadership often doesn't have time for detailed dashboards. The one-pager gives them the essential information they need, quickly and clearly. Stop fighting for budget and start proving your value with hard data. This one-pager is your proof!

Step 5: See how Expel can help you level up

Fantastic! You've taken the first step towards data-driven SOC management. You're seeing your metrics, understanding your performance, and proving your value. But what if you could take it further? What if you could offload the burden of 24x7 SOC operations and maintain data-driven insights and continuous improvement? Learn how Expel's MDR service can boost your security operations.

1. Navigate to the "How Expel Can Help" tab.
2. Learn how Expel Managed Detection and Response (MDR) can transform your security: This page compares your monthly metrics to Expel customer averages. It explains how Expel's MDR service can help you improve your SOC operational metrics using your existing security stack, and take the heavy lifting of threat detection and response off your plate, with 24x7 security operations led by Expel's experts.
3. Want to see exactly how much Expel can help? Get your own customized business value assessment. Follow the link to request a custom business assessment to analyze the value Expel MDR can bring to your organization. This ROI assessment is 100% unique to your environment and company.

Why is this important?

Ready to take your security to the next level? Measuring the KPIs of your SOC with this tool is just the start. When you pair these metrics with Expel MDR, you'll get both the insights and the expertise to strengthen your security program. Ready to do more than just measure? Expel is your partner. Stop just managing—start dominating the threat landscape.

The SOC metrics and KPIs this tool helps you track

To effectively measure SOC performance, it's essential to track a variety of metrics and KPIs across four key categories:

- Analyst workload
- Analyst efficiency
- Incident response & alert lifecycle
- Detection efficacy

Analyst workload metrics

Are your analysts drowning, or just treading water? You can't optimize what you can't see. Understanding your security analyst workload isn't just good management, it's essential for a high-performing SOC. These metrics shine a light on the true demands facing your team, empowering you to intelligently allocate resources, proactively prevent analyst burnout (because burned-out analysts miss things), and ensure your SOC is always ready for what's next. Month-over-month workload tracking isn't just a report; it's your early warning system for resource gaps and a clear path to data-driven staffing decisions.

Metric	Description	How it's calculated	Why it Matters	Industry Benchmark
Est. monthly SOC analyst operating costs	The estimated monthly cost of operating the SOC, including salaries, benefits, and overhead.	Sum the Overall Target Earnings (salaries, benefits, overhead, etc.) of all SOC analysts divided by 12 months in a year.	Helps you understand the financial resources required to run the SOC and identify potential areas for cost optimization. We suggest tracking this month-over-month to track spending trends, identify potential cost overruns, and ensure that the SOC is operating within budget.	
SOC capacity hours	The total number of hours available for the SOC team to work on security-related tasks each month.	Multiply the number of analysts by the number of working labor hours per analyst per month.	Helps you understand the SOC's capacity to handle the workload and identify potential staffing needs. We suggest tracking this month-over-month to understand how the SOC's capacity is evolving over time and whether it aligns with the organization's needs.	

Analyst gross utilization rate	The percentage of an analyst's total working hours spent on productive, billable work.	Divide the total time it takes for analysts to triage alerts, investigate incidents, and handle response by the total available capacity hours for your analysts.	Measures the efficiency of SOC analysts and helps identify potential areas for improvement in resource allocation. We suggest tracking this month-over-month to identify trends in analyst workload, potential burnout, and areas for process improvement.	Target a real-world productivity ratio of 70% to account for breaks, meetings, and other non-task-related activities (Expel)
Additional analyst headcounts needed	The number of SOC analysts needed to maintain continuous 24x7 operations while achieving the target utilization rate.	Divide the total required capacity hours for 24x7 operations by the average number of hours worked per analyst per month at a 70% utilization rate, and subtract the current SOC analyst count.	Helps you plan for staffing needs to ensure 24x7 coverage and avoid analyst burnout. We suggest tracking this month-over-month to adjust staffing plans based on changes in workload, threat landscape, and operational needs.	The minimum requirement for 24x7 SOC operations is 8 analysts. Noisier environments or high-profile companies (and those in industry verticals more prone to attacks) will need to staff more analysts.
Monthly OLA success	The percentage of Operational Level Agreements (OLAs) met each month.	Divide the number of OLAs met by the total number of incidents.	Measures the effectiveness of internal processes and collaborations within the SOC. We suggest tracking this month-over-month to track the consistency of internal processes and identify areas for improvement in collaboration and efficiency.	

Analyst efficiency metrics

Efficiency isn't just a buzzword, it's the bedrock of SOC ROI. Are you getting the most out of every analyst hour? Measuring SOC analyst efficiency isn't about micromanagement; it's about maximizing the value of your security investment. These metrics expose how effectively your team is using their time, pinpoint process roadblocks that are slowing them down, and flag key opportunities for automation to supercharge your operations. Month-over-month tracking isn't just performance

reviews; it's your roadmap to eliminating bottlenecks, optimizing workflows, and driving your SOC to peak performance and maximum efficiency.

Metric	Description	How it's calculated	Why it Matters	Industry Benchmark
Total Alerts Per Month	The total number of security alerts generated by the SOC's detection systems each month.	Sum the number of alerts generated by all security tools and systems used by the SOC.	Provides insights into the level of threat activity and the effectiveness of the SOC's detection capabilities. We suggest tracking this month-over-month to monitor the volume of security alerts and identify any trends or anomalies that may indicate changes in threat activity or detection effectiveness.	
Total time spent on alert triage	The total time spent by SOC analysts triaging security alerts each month.	Multiply the total alerts per month by the average time it takes to triage an alert.	Helps you understand the workload associated with alert triage and identify potential areas for process improvement or automation. We suggest tracking this month-over-month to monitor the efficiency of alert triage processes and identify trends in alert volume and complexity.	Average 10 mins for each security alert triage (Axonius)
Cost of Alert triage	The estimated monthly cost of triaging security alerts.	Multiply the total time spent on alert triage by the average hourly cost of a SOC analyst.	Helps you understand the financial impact of alert triage and identify potential areas for cost optimization. We suggest tracking this month-over-month to track the cost of alert triage and identify potential areas for cost reduction through automation or process improvement.	

True Threats	The number of alerts that are confirmed to be actual security threats (true-positives)	Sum the number of manually reviewed and validated security alerts that are confirmed as actual threats	Helps you understand the true level of risk facing the organization and the effectiveness of the SOC's threat detection capabilities. We suggest tracking this month-over-month to track the actual number of threats and assess the accuracy of threat detection systems to identify areas for improvement and reduce false positives.	
Estimated monthly time investigating true threats	The estimated total time spent by SOC analysts investigating and responding to true threats.	Sum the total time spent by analysts on each true threat.	Helps you understand the workload associated with handling true threats and identify potential areas for process improvement. We suggest tracking this month-over-month to monitor the time spent on investigating true threats and identify trends in incident complexity and resource allocation.	
Estimated cost to investigate true positive threats	The estimated monthly cost of investigating and responding to true threats.	Multiply the estimated total hours spent handling true threats by the average hourly cost of a SOC analyst.	Helps you understand the financial impact of true threats and identify potential areas for cost optimization. We suggest tracking this month-over-month to track the cost of investigating true threats and identify potential areas for cost reduction through automation or process improvement.	
Number of non-threats (False Positives/Benign)	The number of alerts analysts investigated that are incorrectly identified as threats (benign or false-positives)	Sum the number of manually reviewed and validated security alerts that turned out to be benign or false-positive threats.	Helps you understand the accuracy of the SOC's detection systems and identify potential areas for improvement. We suggest tracking this month-over-month to monitor the number of false positives and identify trends or patterns that may indicate issues	Estimated between 41%-80% of alerts are false-positives (SANS 2024 Detection & Response Survey)

			with detection rules or alert tuning.	
Estimated monthly time investigating non-threats	The estimated total time spent by SOC analysts investigating non-threats (false positives).	Sum the time spent by analysts on each benign or false-positive investigation.	Helps you understand the amount of time wasted on investigating false positives and identify potential areas for improvement in alert tuning and automation. We suggest tracking this month-over-month to monitor the time wasted on false positives and identify trends in false positive rates and their impact on analyst workload.	Security teams believe they spend this much time per week on false-positive alerts: <ul style="list-style-type: none"> • 5% – 0 hours • 30% – 1-10 hours • 26% – 11-20 hours • 20% – 21-30 hours • 12% – 31-40 hours • 4% – 41-50 hours • 1% – 51-60 hours • 1% – 60+ hours (Voice of SecOps 4th edition, 2023: Deep Instinct)
Estimated cost to investigate non-threats	The estimated average monthly cost of investigating non-threats (false positives).	Multiply the estimated total hours spent handling non-threats by the average hourly cost of a SOC analyst.	Helps you understand the financial impact of false positives and identify potential areas for cost optimization. We suggest tracking this month-over-month to track the cost of investigating false positives and identify potential areas for cost reduction through automation or process improvement.	
Alerts closed by automation	The number of alerts that are automatically closed by the SOC's security tools and systems.	Sum of all alerts that are automatically closed by security tools and systems.	Measures the effectiveness of automation in reducing the workload of SOC analysts. On average, the use of AI and automation accelerated identification for breaches by 43% for prevention and 33% for response (IBM Cost of a Data Breach Report 2024) . We suggest tracking this month-over-month to monitor the effectiveness of automation in reducing manual effort and identify areas for further automation.	

Estimated cost savings due to automation	The estimated monthly cost savings from using automation to triage alerts.	Multiply the number of alerts closed by automation by the average cost of manually triaging an alert.	Helps you understand the financial benefits of automation in the SOC. We suggest tracking this month-over-month to track the financial benefits of automation and identify areas where automation can be further leveraged to reduce costs.	
--	--	---	---	--

Incident response & alert lifecycle metrics

Seconds matter in a security incident. Are you measuring them? Fast, effective incident response isn't just a "nice to have" – it's the core function of your SOC and your last line of defense against serious damage. These metrics are your stopwatch and performance analyzer for incident response, revealing critical bottlenecks, guiding workflow optimization, and ultimately helping you shrink the blast radius of every attack. Month-over-month tracking isn't just historical data; it's your report card on incident readiness, your validation of process improvements, and your proof that your SOC is built for speed and impact.

Metric	Description	How it's calculated	Why it Matters	Industry Benchmark
Mean time to detect (MTTD)	The average time it takes for the SOC to detect a security incident.	Sum of time to detect all incidents divided by the total number of incidents detected.	A lower MTTD indicates a more proactive SOC that can identify threats before they cause significant damage. We suggest tracking this month-over-month to identify trends in threat detection efficiency and proactively address potential delays or gaps in security monitoring.	

Mean time to acknowledge (MTTA)	The average time it takes for the SOC to acknowledge a security alert.	Sum of the total time to acknowledge all incidents divided by the total number of incidents that must be acknowledged.	Measures the responsiveness of the SOC team to security alerts. We suggest tracking this month-over-month to monitor the team's responsiveness to alerts and identify potential bottlenecks in alert processing or prioritization.	10 minutes to 1 hour (Prophet Security)
Mean time to respond (MTTR)	The average time it takes for the SOC to respond to a detected incident.	Sum of the total time spent responding to and resolving incidents divided by the total number of incidents that required response.	A shorter MTTR means that the SOC can mitigate threats quickly, reducing the potential impact on the organization. We suggest tracking this month-over-month to track the efficiency of incident response processes and identify areas for improvement to expedite threat mitigation.	Suggested Targets: <ul style="list-style-type: none"> • Critical: 1 hour • High: 2 hours • Medium: 4 hours • Low: 8 hours (Prophet Security) In reality, SANS research found organizations respond to confirmed threats: <ul style="list-style-type: none"> • 8.3% within seconds • 41.4% within minutes • 32.8% within hours • 7.8% within a day • 4.6% in multiple days (SANS 2024 Detection & Response Survey)
Mean time to remediate (MTTRm)	The average time it takes for the SOC to remediate a security incident.	Sum of the total time taken to remediate all incidents divided by the total number of incidents remediated.	Measures the efficiency of the SOC's incident remediation processes. We suggest tracking this month-over-month to monitor the effectiveness of remediation efforts and identify any recurring issues or challenges in fully resolving incidents.	
Mean time to mitigate (MTTM)	The average time it takes for the SOC to mitigate the impact of a security incident.	Sum of the total time taken to mitigate all incidents divided by the number of incidents mitigated.	Measures the SOC's ability to reduce the impact of security incidents on the organization. We suggest tracking this month-over-month to assess the SOC's ability to minimize the impact of security incidents and identify areas for	

			improvement in containment and recovery strategies.	
Mean time to identify (MTTI)	The average time it takes for the SOC to detect and acknowledge a security incident.	Sum of Mean times to Detect (MTTD) and Acknowledge (MTTA).	Measures the SOC's ability to detect and validate threats early. We suggest tracking this month-over-month to track the SOC's ability to move from detection to investigation quickly.	194 days (IBM Cost of a Data Breach Report 2024)
Mean time to contain (MTTC)	The average time it takes for the SOC to contain a security incident, preventing it from spreading and causing further damage.	Sum of Mean times to Acknowledge (MTTA) and Respond (MTTR).	Measures the SOC's ability to limit the scope and impact of security incidents. We suggest tracking this month-over-month to track the SOC's ability to contain incidents quickly and effectively, preventing further damage and limiting the scope of the attack.	64 days (IBM Cost of a Data Breach Report 2024)
Mean time of exposure (MTE)	The average time between when a vulnerability is first exploited and when it is mitigated.	Sum of the Mean times to Detect (MTTD), Acknowledge (MTTA), and Respond (MTTR).	Calculated by subtracting the time of mitigation from the time of initial exploitation, and then averaging this value across all incidents. We suggest tracking this month-over-month to track the organization's overall security posture and identify areas for improvement to reduce exposure to threats.	258 days (IBM Cost of a Data Breach Report 2024)
Mean time to close	The average time it takes for the SOC to close a security incident.	Sum of the Mean times to Acknowledge (MTTA), Respond (MTTR), Remediate (MTTRm), and Mitigate (MTTM).	Measures the overall efficiency of the SOC's incident response process. We do not suggest using this as your overall measurement since this can lead to encouraging analysts to closing alerts and incidents faster to "game" the system (hit a number) rather than focusing on	

			<p>security and thoroughness of the response and remediation process.</p> <p>We suggest tracking this month-over-month to monitor the overall efficiency of the incident response process from detection to closure, identifying areas for improvement in each stage.</p>	
--	--	--	---	--

Detection efficacy metrics

Garbage in, garbage out. Is your threat detection actually detecting threats? A strong security posture starts with rock-solid threat detection. These metrics are your truth serum for your SOC's detection capabilities, revealing blind spots in your coverage, guiding precision tuning of detection rules, and helping you silence the noise of false positives while ensuring you never miss a real threat.

Month-over-month tracking isn't just system logs; it's your ongoing health check for your detection systems, highlighting critical areas for improvement, and guaranteeing your SOC is focused on what actually matters: real threats.

Metric	Description	How it's calculated	Why it Matters	Industry Benchmark
Alert precision	The number of security alerts that escalated into actual security incidents.	Divide the number of true positives by the sum of true-positives, false-positives, and benign alerts.	<p>Helps you understand the correlation between alerts and incidents and identify potential areas for improvement in alert triage and detection engineering/tuning. This answers the question, "Of all the instances labeled as positive, how many are actually positive?"</p> <p>We suggest tracking this month-over-month to track the effectiveness of alert triage and incident response processes, identifying any areas where improvements can be made to prevent alerts</p>	

			from escalating into incidents.	
Detection efficacy rate	The percentage of alerts that are incorrectly identified as threats.	Divide the number of false-positive alerts by the total number of alerts generated	A high false positive rate can overwhelm SOC analysts and lead to alert fatigue, whereas a low rate indicates more accurate threat detection. We suggest tracking this month-over-month to track the accuracy of threat detection systems and identify areas for improvement to reduce false positives.	Critical: <25% High: <50% Medium: <75% Low: <90% (Prophet Security)
Monthly detections create	The number of new security detections created by the SOC each month.	Sum the number of new detection rules or signatures created by the SOC and/or Detection Engineering teams	Measures the SOC's ability to proactively identify and respond to new threats. We suggest tracking this month-over-month to measure how effectively your detection engineering team is able to create new detections as new threats emerge and new TTPs are discovered.	
Detection creation turn-around time	The average time it takes for the SOC to create and deploy a new detection rule or signature.	Estimate the time it takes for your team to create and deploy a new detection when a new attacker tactic, technique, and procedure (TTP) is discovered.	Measures the SOC's agility in responding to new threats. We suggest tracking this month-over-month to monitor the efficiency of the detection development process and ensure that new detections are deployed quickly to address emerging threats.	

DISCLAIMER: This SOC Metrics & Efficiency KPIs Dashboard (the "Tool") is provided by Expel, Inc. ("Expel") for informational purposes only and does not constitute professional advice. You are solely responsible for any decisions you make based on the use of this Tool. Exporting data may lead to errors; Expel is not responsible for issues arising from exporting data to other file types. This Tool does not reflect the capabilities of the Expel MDR service. Expel provides this Tool "AS IS" and without any warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, or non-infringement. Expel is not responsible for any errors, omissions, or inaccuracies in the Tool or any damages resulting from its use. The team at Expel built the underlying financial model for this Tool based on industry defined metrics and KPIs. All calculations are listed in the "Calculations" hidden tab. If you find a discrepancy in the calculations, please email Expel for assistance and/or troubleshooting at marketingtools@expel.com.