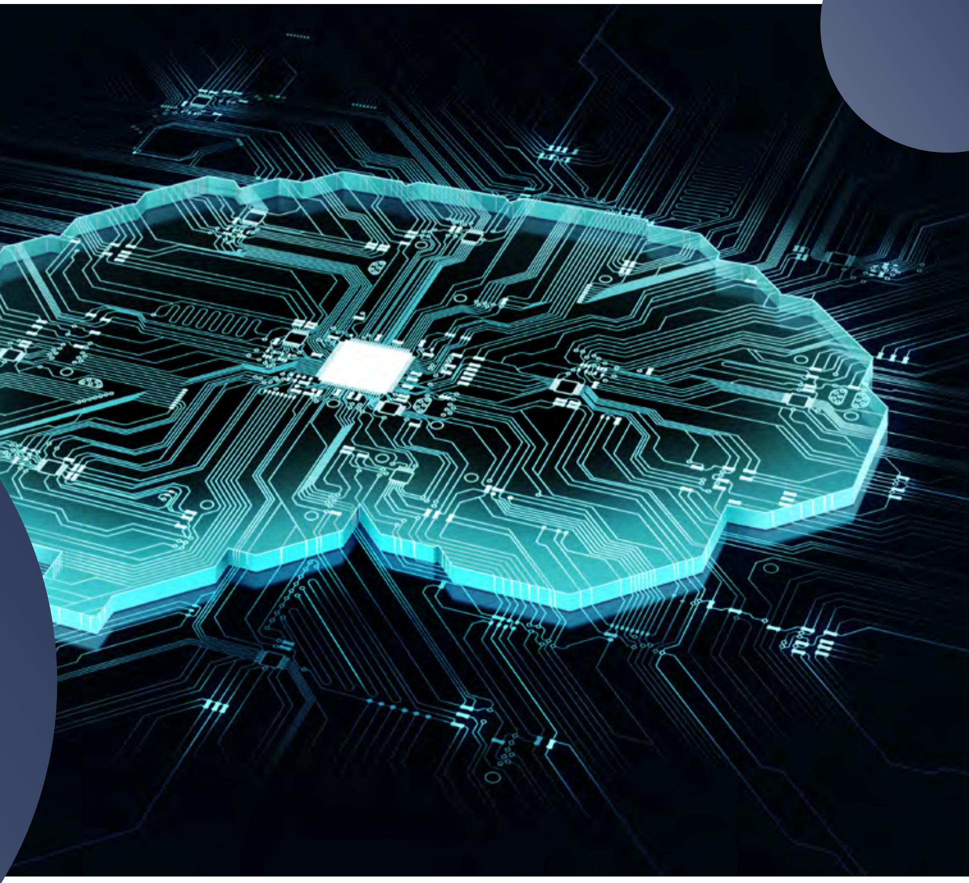
HiveWatch



Your Guide to: AI in the GSOC

How security operations centers are benefiting from innovative tech (and how to get started in your program)

As security programs mature beyond "gates, guards, and guns," leaders are turning toward comprehensive technology innovations to drive change. In many companies with centralized management of security, operations centers – often called security operations centers (SOCs) or global SOCs (GSOCs) – are responsible for protecting people, assets, and operations. However, traditional operational models that are unsustainable in their current state are a massive challenge to overcome.

Enter: artificial intelligence (AI)-enabled technology.

GSOCs stand to become one of the primary benefactors of AI technology, as resourcing continues to be a major challenge for security leaders to overcome.

In this guide, we explore how AI is transforming security operations and provide practical insights for security professionals looking to effectively leverage AI technology across the enterprise.

WHAT IS A SECURITY OPERATIONS CENTER?

A SOC or GSOC can be considered the central nervous system of an organization's physical security infrastructure. The common task for a GSOC is monitoring and responding to security events on a regional or global scale. Typically, a GSOC operates 24/7, coordinating emergency responses and managing various security systems, such as:

- Video surveillance systems
- Access control platforms
- Intrusion detection systems
- Emergency communication networks
- Guard force management
- Incident response coordination

Typical GSOCs serve as a centralized place for incoming security data related to the above systems to be collected, analyzed, and acted on. More specifically, a GSOC integrates intelligence from various sources to better facilitate response in the event of a security incident or emergency.

GSOCs act as a core function for mitigating risk to an organization, protecting assets and people from harm, and maintaining awareness of multiple locations and the risks they face.

GSOCs play a multitude of roles, including:

- Monitoring the performance of cameras and access control point solutions to ensure the availability and continuous flow of data
- Communicating with internal and external security personnel (guarding resources, resource officers, local law enforcement) in the event of an emergency or incident
- Facilitating emergency response protocols
- Ensuring the safety and security of people, brands, and assets
- Providing valuable insights about the performance of an organization's security program using actionable intelligence
- Gathering data from multiple sources to better inform response through intelligence-driven decision-making

3 SECURITY OPERATIONS CHALLENGES TO OVERCOME

Today's GSOCs face unique challenges within the frame of reference for their own organization or vertical market – i.e., regulatory compliance, multi-region visibility, and multiple third-party agencies across the enterprise. Still, three common challenges can be seen across the board, no matter what business you're in:

Resourcing

The biggest challenge for security leaders managing an internal GSOC is resourcing and keeping the facility staffed 24/7. Budget limitations can mean trying to do more with fewer people. And in the guarding and operator world, high turnover rates can wreak havoc on a department's ability to adequately staff a GSOC (some studies show that positions like these have a 100% to 300% turnover rate annually, and it costs a lot of money and time to train incoming resources).

Operational Inefficiencies

While resourcing is a critical piece, the challenges of training new operators can be exacerbated by the overwhelming number of platforms that these individuals are tasked with monitoring. Not only that, there's an insane number of video feeds and alarms that require ongoing monitoring. High false alarm rates can also mean alarm fatigue can set in, which might lead to missed events that can be dangerous. In so many GSOCs, the highly manual nature of assessing incoming alarms and elevating as needed can take a lot of time and energy from operators throughout their shifts, which can lead to delayed response times. Finally, the differences from one SOC to the next can mean inconsistencies related to security protocols (and the inability to know the next steps in the event of an incident).

More Security Demands

Organizations understand that the safety and security of people and assets are essential, which means the function of the GSOC is more important than ever. The increasing numbers of incidents that demand attention from various threat categories mean that security teams are navigating even more demands on their time. The nature of threats is also changing with more complex facility breakdowns and more point solutions to monitor. The same facilities are also tasked with ensuring that regulatory compliance requirements are met and that all of the investments being made in new equipment or additional resources are leading to a return on investment (ROI) for the business (and so much of this is tied to decision-making around NEW investments, too).

These challenges are leading to a critical breaking point for security leadership, who are beginning to explore different ways to solve some of these issues by investing in technology that enables better response and management. Sometimes, this might mean thinking completely outside the box and considering AI-driven tech.

PHYSICAL SECURITY'S ROLE

As the world changes, physical security continues to be a growing need, yet companies struggle with high operational costs and inefficiencies.

Organizations are being asked to do more with less, and program dollars need to stretch further, meaning that security leaders have to change the way businesses view the role of physical security.

Physical security can reduce risk, increase safety, and drive overall impact on the business. Instead of seeing physical security as a necessity, it can be viewed as a strategic asset.

Physical security has been overshadowed by cybersecurity in recent years but is a vital contributor to the protection of a company's people, assets, and brand. Mitigating risk and ensuring safety has been, and will always be, a C-level initiative.

In fact, the physical security industry is projected to reach $171.4 billion in annual growth by 2028.

So what is the majority of this spent on? People. In the U.S., hourly wages for security operators typically range from $20 to $40, depending on experience and location. For each operator, it takes anywhere from a few weeks to several months, depending on complexity and the operator's existing skill level, to get trained and ready to go. Then comes the real kicker: while turnover isn't unique to any industry, the security industry (specifically, security operators and officers) has an astronomically high turnover rate, with national annual rates of anywhere from 100-300%. So now an organization has spent all this time, money, and resources ... to have to start over again.

On top of this, security teams are drowning in video feeds and alarms, so they continue to throw people at the problem to catch up. Security operators are inundated with repetitive and mundane tasks, tying them down with low-impact, time-consuming work. This type of activity creates intense frustration, leading to complacency, burnout, and high turnover, and is ultimately a waste of company funds and resources.

HOW AI HELPS

All of this to say the physical security industry, with huge budgets to spend and C-level eyes on risk, is due for a technology disruption, and AI is the answer.

The addition of AI-driven technology that is actually feasible for organizations to adopt (meaning, it can be actually transformative from an operational perspective) is set to push digital transformation even further across the entire organization. Physical security done right can and will produce an ROI, as security teams can now focus more on high-value, more complex strategic initiatives, such as business continuity and supply chain resilience, instead of alarm-chasing.

The growth in AI has already proven to be useful and successful in the cybersecurity realm. Cybersecurity tools leverage AI to process and analyze large volumes of data in real-time. This technology allows organizations to detect and respond to threats more swiftly and effectively than

relying solely on human analysis. By employing advanced algorithms and pattern recognition methods, AI-driven security systems can pinpoint anomalies, suspicious behaviors, and potential vulnerabilities that human operators might overlook and allow humans to fix the potential issues before they become significant threats.

In physical security applications, similar outcomes can be achieved. The advances in machine learning and computer vision, the accessibility of AI technology, and the growing need for automated threat detection mean that AI is a natural fit to help address some of the resourcing, operations, and security challenges we mentioned in this guide.

AI APPLICATIONS IN THE GSOC

The integration of AI into GSOCs represents a significant shift in how security teams operate and respond to threats. Modern AI systems can simultaneously process vast amounts of data from multiple sources, identifying patterns and potential threats that human operators might miss. These systems excel at handling routine tasks such as monitoring video feeds, verifying alarms, and executing standard operating procedures, allowing human operators to focus on complex decision-making and strategic security initiatives.

Video applications

In surveillance operations, AI systems continuously monitor multiple video feeds, detecting and classifying objects, people, and behaviors in real time. These systems can identify suspicious activities such as loitering, abandoned objects, or unauthorized access attempts, automatically alerting operators to potential threats. AI's ability to maintain consistent vigilance across numerous cameras simultaneously dramatically expands the effective coverage area of security operations without requiring additional human resources.

Alarm management

Traditional security systems often generate high volumes of false alarms, leading to operator fatigue and potentially missed threats. AI systems can intelligently filter and verify alarms, analyzing multiple data points to determine the likelihood of a genuine security threat.

AI-driven technology is changing the way teams do:

- Real-time video analysis and threat detection
- Automated alarm verification and triage
- Pattern recognition and anomaly detection
- Intelligent dispatch and response coordination
- Automated report generation and documentation

This intelligent triage ensures that operators focus their attention on the most critical incidents, improving response times and reducing the risk of alarm fatigue.

Incident response and management

When an incident occurs, AI systems can automatically gather relevant data from multiple sources, including video feeds, access control logs, and sensor data. The system can generate preliminary incident reports, dispatch appropriate personnel according to established protocols, and maintain a detailed record of all actions taken. This automation ensures consistent application of security procedures while creating comprehensive documentation for future analysis and compliance purposes.

Data-driven decision-making

By analyzing historical data and identifying patterns, AI systems can help predict potential security risks before they materialize. This includes identifying unusual access patterns, detecting anomalies in foot traffic, or recognizing behavioral patterns that indicate future security threats. These insights enable security teams to take proactive measures rather than merely responding to incidents after they occur.

IMPLEMENTATION CONSIDERATIONS

Technology Requirements

Successfully implementing AI in a GSOC requires careful consideration of the underlying technical infrastructure. The foundation begins with high-performance computing infrastructure capable of processing vast amounts of data in real time. This includes powerful servers and workstations that can handle concurrent video streams, complex AI algorithms, and multiple integrated security applications without performance degradation.

Network infrastructure plays an equally critical role, as AI-enabled security systems demand robust, reliable connectivity with sufficient bandwidth to handle continuous data streams from multiple sources. Organizations must ensure their network architecture can support real-time video processing, data analysis, and system integration while maintaining redundancy for critical operations. This often involves upgrading existing networks and implementing failover systems to prevent service interruptions.

Integration capabilities represent another crucial technical consideration. Modern GSOCs typically operate multiple security platforms, including video management systems (VMS), access control systems, and incident management software. AI solutions must seamlessly integrate with these existing systems while maintaining compatibility with legacy infrastructure. This requires careful evaluation of API availability, integration protocols, and system architecture to ensure smooth data flow between platforms.

Data management infrastructure forms the backbone of AI operations. Organizations must implement robust storage solutions capable of handling large volumes of security data, including video footage, event logs, and AI-generated analytics. This involves establishing appropriate data retention policies, implementing backup systems, and ensuring proper data security measures are in place. Additionally, organizations need to consider scalability requirements as their security operations grow and evolve.

Management Considerations

When implementing AI in the GSOC (or anywhere in the organization), leadership should establish clear oversight structures that define roles, responsibilities, and decision-making processes for AI-assisted operations. This includes developing comprehensive policies governing AI system use, data handling procedures, and compliance requirements (pro tip: talk to your legal department about what's acceptable before you sign any contracts). Security leaders should create detailed frameworks that outline how AI systems integrate with existing security operations while maintaining appropriate human oversight.

Organizations must carefully document how AI tools integrate into existing workflows, including specific procedures for system monitoring, incident response, and escalation protocols. These standard operating procedures (SOPs) should clearly delineate the roles of AI systems and human operators, establishing clear guidelines for using AI-driven decisions and escalation versus when human intervention is required.

Training and development programs become increasingly critical with AI implementation. Security personnel require comprehensive training in operating AI systems and understanding their capabilities and limitations. This includes developing new skill sets for data analysis, system monitoring, and incident investigation using AI tools. Organizations should implement ongoing training programs that keep pace with system updates and evolving security requirements while ensuring operators maintain proficiency in both AI-assisted and manual operations.

Cost Factors

ROI measurement becomes even more important as organizations invest in AI technology. Security leaders must develop comprehensive metrics for evaluating system performance and business impact. This includes tracking direct cost savings from reduced false alarms, improved operator efficiency, and decreased incident response times. When calculating overall return on investment, organizations should also consider indirect benefits such as improved security coverage, reduced liability exposure, and enhanced compliance capabilities.

3 BENEFITS OF AI-ENABLED GSOCS

Operational Improvements

Using AI technology in an organization's GSOCs can impact security operations across the enterprise. One of the most immediate and measurable impacts is the dramatic reduction in false alarm rates. AI systems can analyze multiple data points simultaneously to verify potential threats, filtering out false positives that traditionally consume valuable operator time and resources. This intelligent filtering ensures that security teams focus their attention on genuine security threats rather than chasing false alarms.

Response times also see marked improvement. When incidents occur, AI systems can instantly assess the situation, categorize the threat level, and initiate appropriate response protocols without human delay. This automated triage and initial response capability ensures that critical incidents receive immediate attention while maintaining consistent handling of routine events. The system's ability to monitor multiple feeds and incidents simultaneously ensures no security events go unnoticed, regardless of concurrent activity levels.

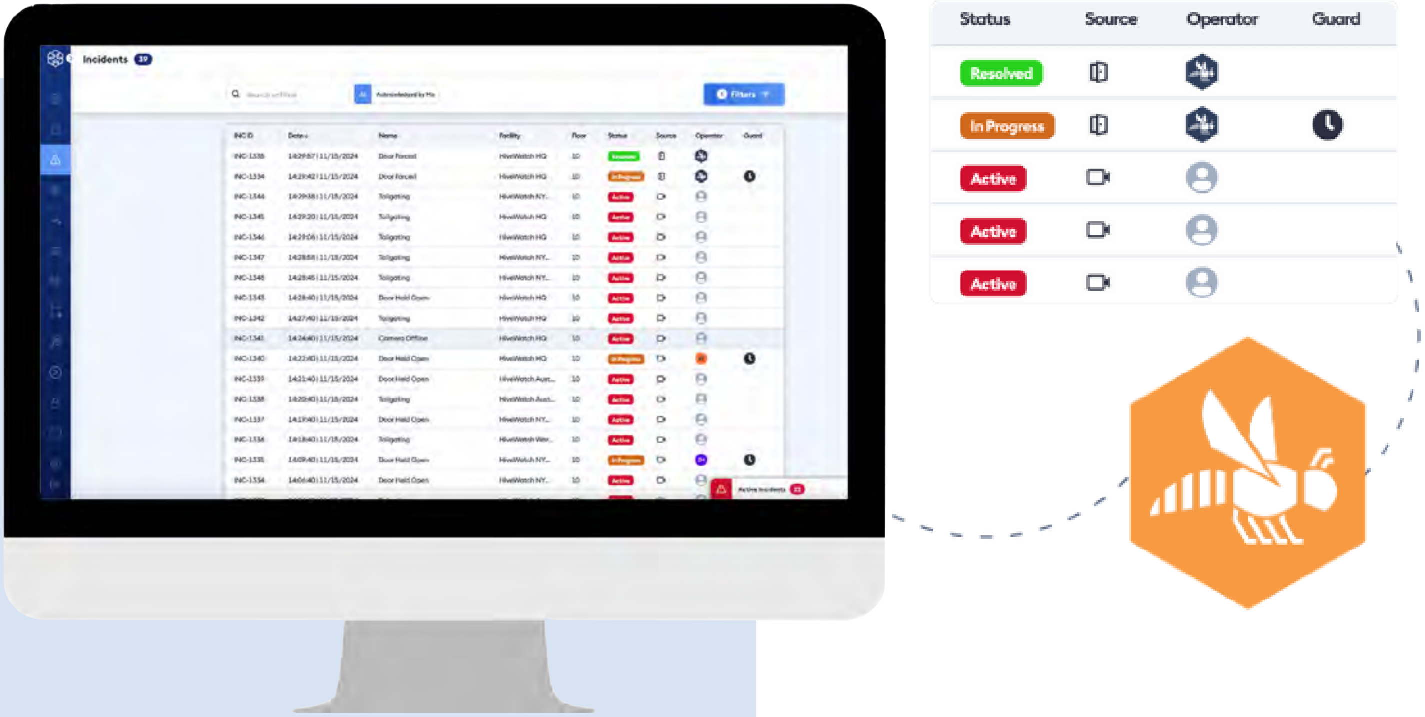
Protocol applications become more consistent and reliable through AI automation. Standard operating procedures are executed uniformly across all incidents, ensuring consistency across the enterprise. This standardization means that every incident receives the appropriate attention and follows established security protocols, regardless of the time of day or operator workload. The system maintains detailed documentation of all actions, creating a comprehensive audit trail for future reference and analysis.

Resource allocation improves significantly with AI-enabled operations. The system can intelligently distribute workload based on incident priority, operator availability, and specific expertise requirements. This dynamic resource management ensures optimal coverage while preventing operator overload. Additionally, AI systems can predict peak activity periods based on historical data, allowing security teams to adjust staffing levels to meet anticipated demands proactively.

Business Impact

Organizations typically see decreased staffing requirements for routine monitoring tasks, reduced training costs through automated assistance, and lower incident-related expenses through improved prevention and faster response times. The ability to handle increased security coverage without proportional increases in staffing creates significant scalability advantages.

Liability exposure decreases through improved incident documentation and consistent protocol application. AI systems maintain detailed records of all security events, responses, and outcomes, creating comprehensive audit trails that can prove invaluable in legal situations. The system's ability to ensure consistent application of security procedures helps demonstrate due diligence in security operations, potentially reducing legal vulnerability.



INC ID	Date ↓	Name	Facility	Floor	Status	Source	Operator	Guard
INC-1335	14:29:57 | 11/15/2024	Door Forced	HiveWatch HQ	10	Resolved			
INC-1334	14:29:42 | 11/15/2024	Door Forced	HiveWatch HQ	10	In Progress			🕒
INC-1344	14:29:38 | 11/18/2024	Tailgating	HiveWatch NY...	10	Active			
INC-1345	14:29:20 | 11/15/2024	Tailgating	HiveWatch HQ	10	Active			
INC-1346	14:29:06 | 11/15/2024	Tailgating	HiveWatch HQ	10	Active			
INC-1347	14:28:58 | 11/18/2024	Tailgating	HiveWatch NY...	10	Active			
INC-1348	14:28:46 | 11/15/2024	Tailgating	HiveWatch NY...	10	Active			
INC-1343	14:28:40 | 11/15/2024	Door Held Open	HiveWatch HQ	10	Active			
INC-1342	14:27:40 | 11/15/2024	Tailgating	HiveWatch HQ	10	Active			
INC-1341	14:24:40 | 11/15/2024	Camera Offline	HiveWatch HQ	10	Active			
INC-1340	14:22:40 | 11/15/2024	Door Held Open	HiveWatch HQ	10	In Progress			🕒
INC-1339	14:21:40 | 11/15/2024	Door Held Open	HiveWatch Aust...	10	Active			
INC-1338	14:20:40 | 11/15/2024	Tailgating	HiveWatch Aust...	10	Active			
INC-1337	14:19:40 | 11/15/2024	Door Held Open	HiveWatch NY...	10	Active			
INC-1336	14:18:40 | 11/15/2024	Tailgating	HiveWatch Wer...	10	Active			
INC-1335	14:09:40 | 11/15/2024	Door Held Open	HiveWatch NY...	10	In Progress			🕒
INC-1334	14:06:40 | 11/15/2024	Door Held Open	HiveWatch NY...	10	Active			

Status	Source	Operator	Guard
Resolved			
In Progress			🕒
Active			
Active			
Active			

Security coverage expands significantly without proportional cost increases. AI systems can monitor multiple locations simultaneously, maintaining consistent vigilance across all areas. This expanded coverage capability allows organizations to protect larger areas or multiple facilities without requiring proportional increases in security personnel. The system's real-time ability to detect and respond to potential threats enhances overall security effectiveness.

Regulatory compliance becomes more manageable through automated documentation and consistent procedure application. AI systems can be programmed to ensure security operations align with relevant regulations and standards, maintaining detailed compliance records automatically. This automated compliance management reduces the administrative burden on security teams while providing better assurance of regulatory adherence.

Personnel Benefits

The integration of AI technology significantly reduces operator burnout by automating routine and repetitive tasks. Security personnel are freed from the monotony of continuous video monitoring and alarm verification, allowing them to focus on more engaging and strategic activities. This reduction in routine task load helps maintain operator alertness and engagement during critical incidents.

Career development opportunities expand as security roles evolve to incorporate new technologies. Operators gain experience with advanced security systems and develop new data analysis and system management skills. This technological expertise enhances career prospects and provides pathways for professional advancement within the security field. The shift from routine monitoring to strategic security management creates role expansion and specialization opportunities.

Job satisfaction improves as security personnel engage in more meaningful and impactful work. Rather than spending shifts monitoring routine activities, operators can focus on incident investigation, threat assessment, and strategic security planning. This elevation of security roles from monitoring to analysis and decision-making creates more engaging and professionally satisfying positions.

Work-life balance benefits from more efficient resource allocation and reduced stress levels. The consistent support of AI systems helps prevent operator overload during high-activity periods, while automated monitoring reduces the pressure of continuous vigilance. This improved operational environment contributes to better job satisfaction and lower turnover rates among security personnel.

THE FUTURE IMPACT OF AI IN GSOCS

As the physical security industry approaches a projected market size of $171.4 billion by 2028, integrating AI into security operations represents a massive transformation in how organizations approach security. The traditional challenges of high turnover rates, overwhelming monitoring demands, and increasing security threats have created an unsustainable operational model that demands innovation. AI becomes the force multiplier for security teams to do more with less.

Using the technology, organizations can strengthen security coverage without seeing increases in staffing costs while also improving response times and reducing false alarm rates. The consistency and reliability of AI-driven operations enhance compliance capabilities and reduce liability exposure through comprehensive documentation and standardized protocol application, rather than being viewed merely as a necessary cost center, security operations can demonstrate tangible value through improved efficiency, enhanced risk management, and direct contributions to business continuity.

> The future of physical security is in the partnership between human expertise and AI capabilities.

Those security teams that thoughtfully approach AI implementation in their GSOCs will be better able to meet the needs of the enterprise as threats become more sophisticated. This transformation represents an operational improvement and a strategic opportunity to reimagine physical security for the modern era, where technology and human insight combine to create more effective, efficient, and responsive security operations.

To learn more about how HiveWatch is leading the way in the transformation of tangible AI-enabled security operations, click here.

HiveWatch