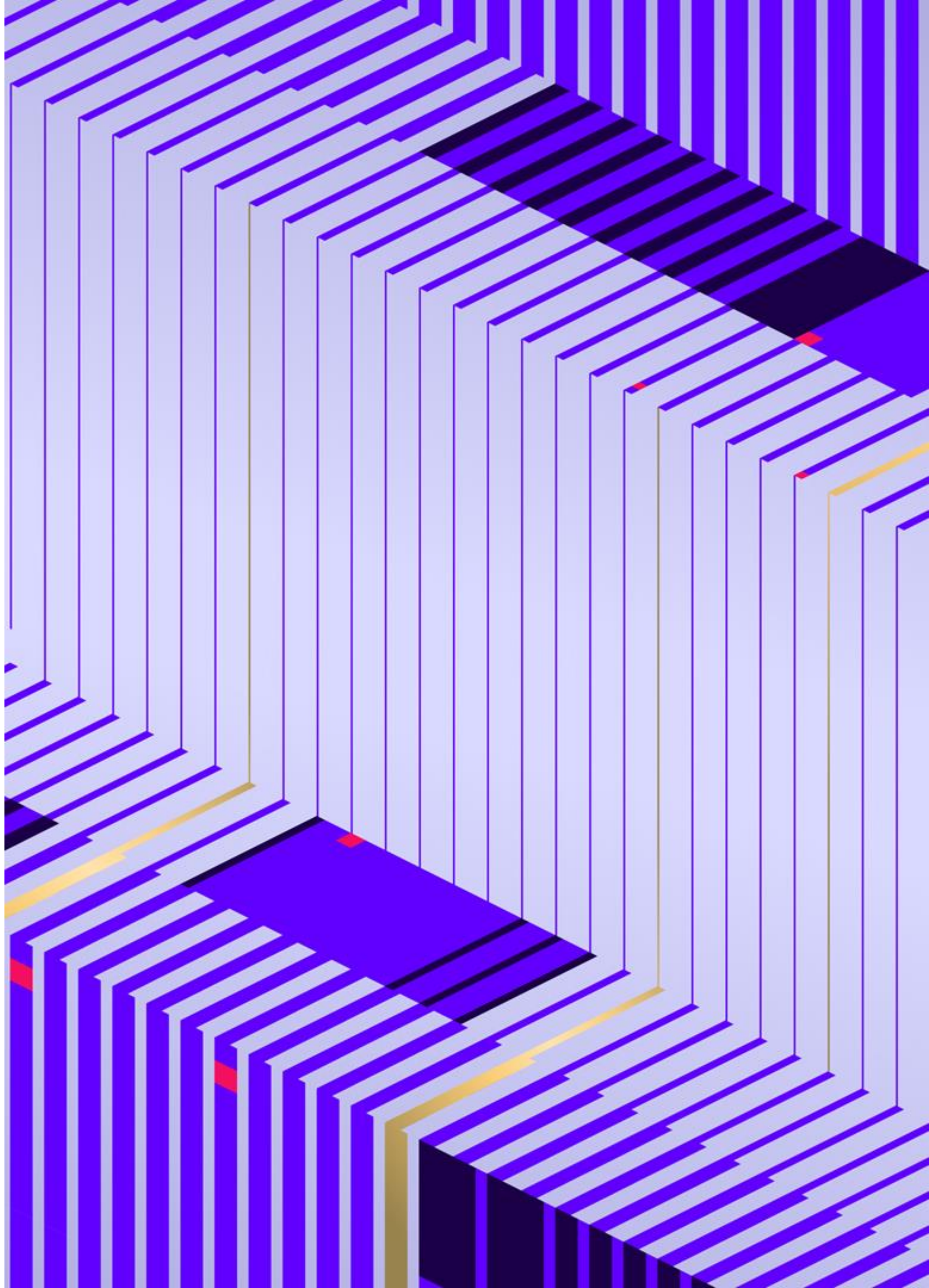
How AI is Driving the Autonomous SOC

Chris Boehm
Global Field CISO

Automating Security Operations to the Point of Autonomy

SentinelOne
Secure Tomorrow



Agenda

- Business Impacts of AI
- From Autonomous Vehicles to Autonomous Security
- Levels of SOC Automation
- Leadership in the Era of AI

SentinelOne

Business Impacts of Artificial Intelligence

The Future of Business is AI-Driven

80%

Percentage of improvement in productivity reported by staff directly using AI technology.

$1.8T

The global AI market is expected to reach over $1.8 trillion by 2030.

73%

Of companies waste time on manual tasks that AI can automate.

92%

Of supply chain execs make gut decisions because their reports don’t provide predictive guidance, which could be achieved through AI.

100%

Of healthcare payer CIOs report that AI and ML tech will be implemented in their systems by 2026.

44%

Of hedge fund managers surveyed by BNP Paribas report they use ChatGPT within their professional work daily.

The Business Value Creation of AI

Intelligent Integrations

Chatbots and Virtual Assistants

AI engines integrate with APIs to create intelligent chatbots and virtual assistants for enhanced support.

Personalized Recommendations

AI engines use ML to provide personalized recommendations for products, content, or services.

Image and Video Analysis

APIs allow apps to analyze and understand content of images and videos for object detection, facial recognition, and scene analysis.

Natural Language Processing (NLP)

APIs provide advanced text analysis, including sentiment analysis, entity recognition, and language translation.

Speech Recognition and Synthesis

APIs convert spoken language into text and vice versa, enabling voice-controlled applications and accessibility features.

Predictive Analytics

Cloud platforms enable developers to build, train, and deploy machine learning models for predictive analytics through API integrations.

Document Processing

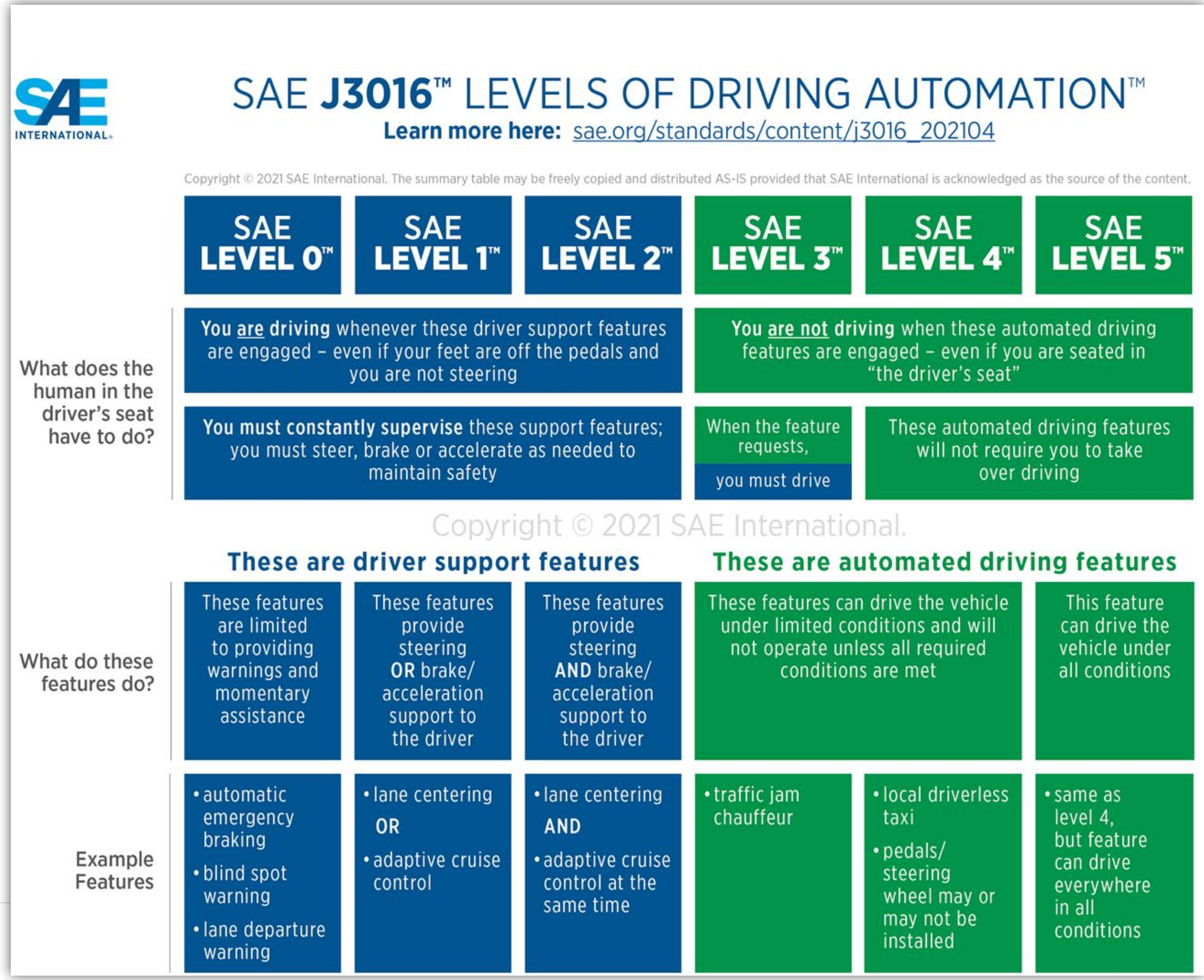
APIs extract structured data from scanned documents, PDFs, and images, automating data entry and document processing tasks.

Fraud Detection

AI can leverage API integrations in payment gateways to analyze transaction patterns and flag suspicious activities in real-time.

From Autonomous Vehicles to Autonomous SOC

SAE International Levels of Driving Automation



SAE **J3016**™ LEVELS OF DRIVING AUTOMATION™

Learn more here: sae.org/standards/content/j3016_202104

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	**You are driving** whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			**You are not driving** when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			**These are automated driving features**		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering **OR** brake/ acceleration support to the driver	These features provide steering **AND** brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering **OR** • adaptive cruise control	• lane centering **AND** • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

Levels of Driving Automation

Level 0

The driver is fully responsible for controlling the vehicle from steering to accelerating and braking.

Level 1

The vehicle can assist using Advanced Driver Assistance Systems (ADAS).

Level 2

The vehicle now can control both steering, acceleration, and parking, but the human driver must remain attentive and ready to take over.

Level 3

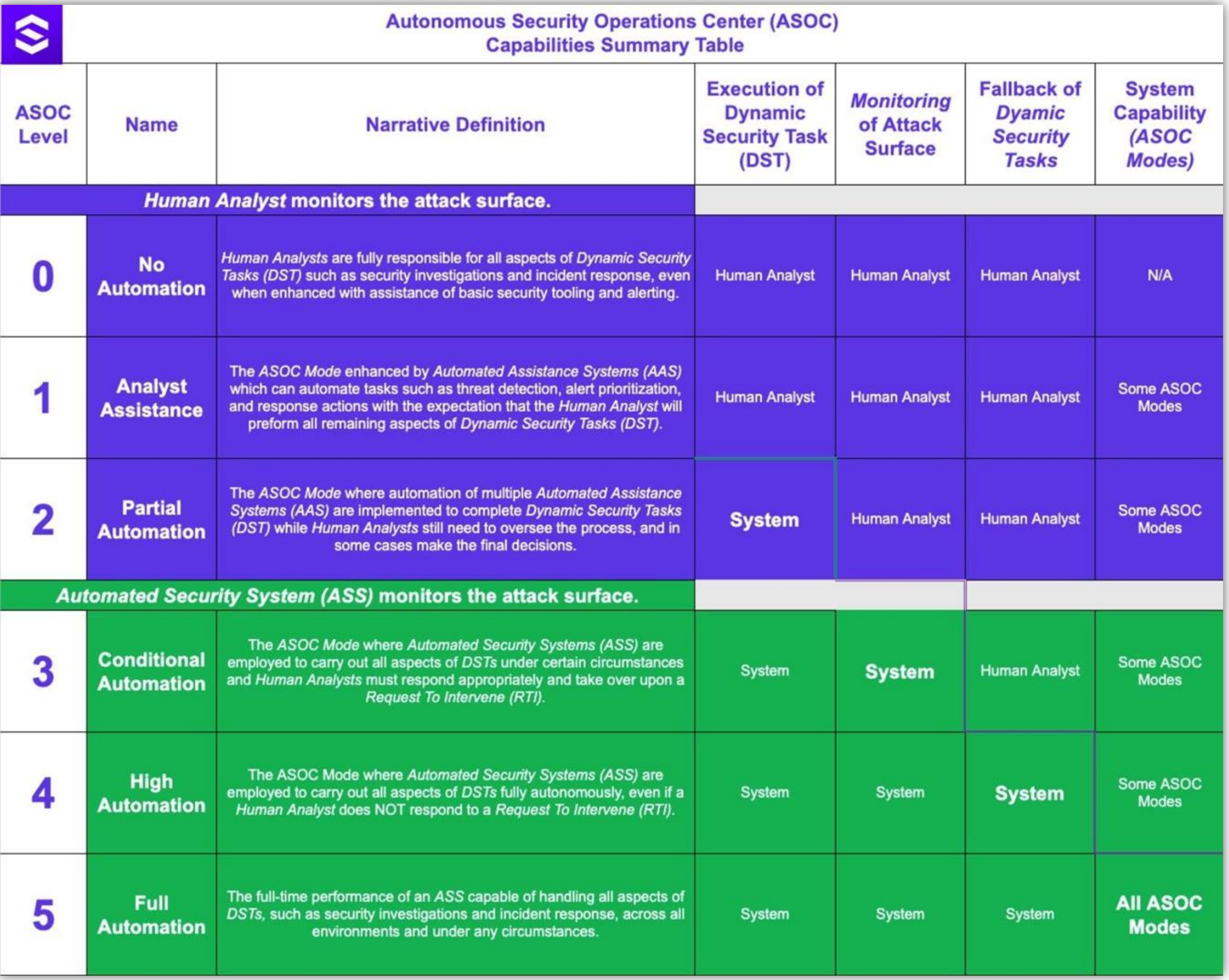
The vehicle manages most driving tasks and even monitors the external environment under certain conditions.

Level 4

The vehicle can perform all driving tasks and monitor the environment in most situations without human intervention.

Level 5

The fully autonomous vehicle can handle all driving tasks in all environments without any human intervention.



Autonomous Security Operations Center (ASOC)
Capabilities Summary Table

ASOC Level	Name	Narrative Definition	Execution of Dynamic Security Task (DST)	*Monitoring* of Attack Surface	Fallback of *Dyamic Security Tasks*	System Capability *(ASOC Modes)*
***Human Analyst* monitors the attack surface.**						
0	No Automation	*Human Analysts* are fully responsible for all aspects of *Dynamic Security Tasks (DST)* such as security investigations and incident response, even when enhanced with assistance of basic security tooling and alerting.	Human Analyst	Human Analyst	Human Analyst	N/A
1	Analyst Assistance	The *ASOC Mode* enhanced by *Automated Assistance Systems (AAS)* which can automate tasks such as threat detection, alert prioritization, and response actions with the expectation that the *Human Analyst* will preform all remaining aspects of *Dynamic Security Tasks (DST)*.	Human Analyst	Human Analyst	Human Analyst	Some ASOC Modes
2	Partial Automation	The *ASOC Mode* where automation of multiple *Automated Assistance Systems (AAS)* are implemented to complete *Dynamic Security Tasks (DST)* while *Human Analysts* still need to oversee the process, and in some cases make the final decisions.	**System**	Human Analyst	Human Analyst	Some ASOC Modes
***Automated Security System (ASS)* monitors the attack surface.**						
3	Conditional Automation	The *ASOC Mode* where *Automated Security Systems (ASS)* are employed to carry out all aspects of *DSTs* under certain circumstances and *Human Analysts* must respond appropriately and take over upon a *Request To Intervene (RTI)*.	System	**System**	Human Analyst	Some ASOC Modes
4	High Automation	The ASOC Mode where *Automated Security Systems (ASS)* are employed to carry out all aspects of *DSTs* fully autonomously, even if a *Human Analyst* does NOT respond to a *Request To Intervene (RTI)*.	System	System	**System**	Some ASOC Modes
5	Full Automation	The full-time performance of an *ASS* capable of handling all aspects of *DSTs*, such as security investigations and incident response, across all environments and under any circumstances.	System	System	System	**All ASOC Modes**

Journey towards the ASOC

Levels of Security Operations Center (SOC) Automation

Level 1: Analyst (aka Driver) Assistance

At Level 1, security analysts must always play an active role in security operations.

Technologies that offer some level of support or automation.

SIEM / SOAR / Hyperautomation Tools

Automate non-investigation, routine tasks.

Data Enrichment / Initial Response

Requires analysts to monitor execution and handle failures.

Basic Scripts / No Situational Awareness

Level 2: Partial Automation

Security systems can automate multiple investigation tasks and even suggest recommended responses.

Automatically respond to incidents based on predefined criteria.

Automated Assistance Systems (AAS)

Analysts set the rules and workflows guided by AI assistance.

Human Oversight / Finał Decision

Correlate alerts, gather context, & recommend responses.

Continual Assistance / Partial Automation

Level 3: Conditional Automation

Autonomously carry out comprehensive security functions under specific conditions.

Autonomously respond based on pre-trained models and historical data.

Automated Security System (ASS)

Analysts required to take over only if the system encounters unexpected situation.

Request To Intervene (RTI)

Generative AI and Large Language Models (LLM) accelerate security operations.

AI-Powered Operations

Automated threat hunting, vulnerability management, and cyber investigations.

Dynamic Security Task (DST)

Level 4: High Automation

Systems capable of fully managing the entire threat lifecycle autonomously.

Deployed in specific environments where the scope of threats are well-defined.

Operational Design Domain (ODD)

Automatically handle multiple investigations, response actions, and concurrent incidents.

Autonomous Security Agents

Significant reduction in human oversight maintaining ability for manual intervention.

Human Override Available

Recovery from malfunctions or issues without human intervention.

Self-Healing Security System

Level 5: Full Automation

Full IT Systems Integration

Integrates with the IT environment providing a unified view of security posture and coordinates defense strategies across the entire infrastructure.

Breach Prediction

Perform complex security analyses and threat modeling that can anticipate potential security issues.

Proactive Threat Hunting

Hunts for novel threats, identifying malicious behavior and neutralizing them before they can cause significant harm.

Fully Autonomous

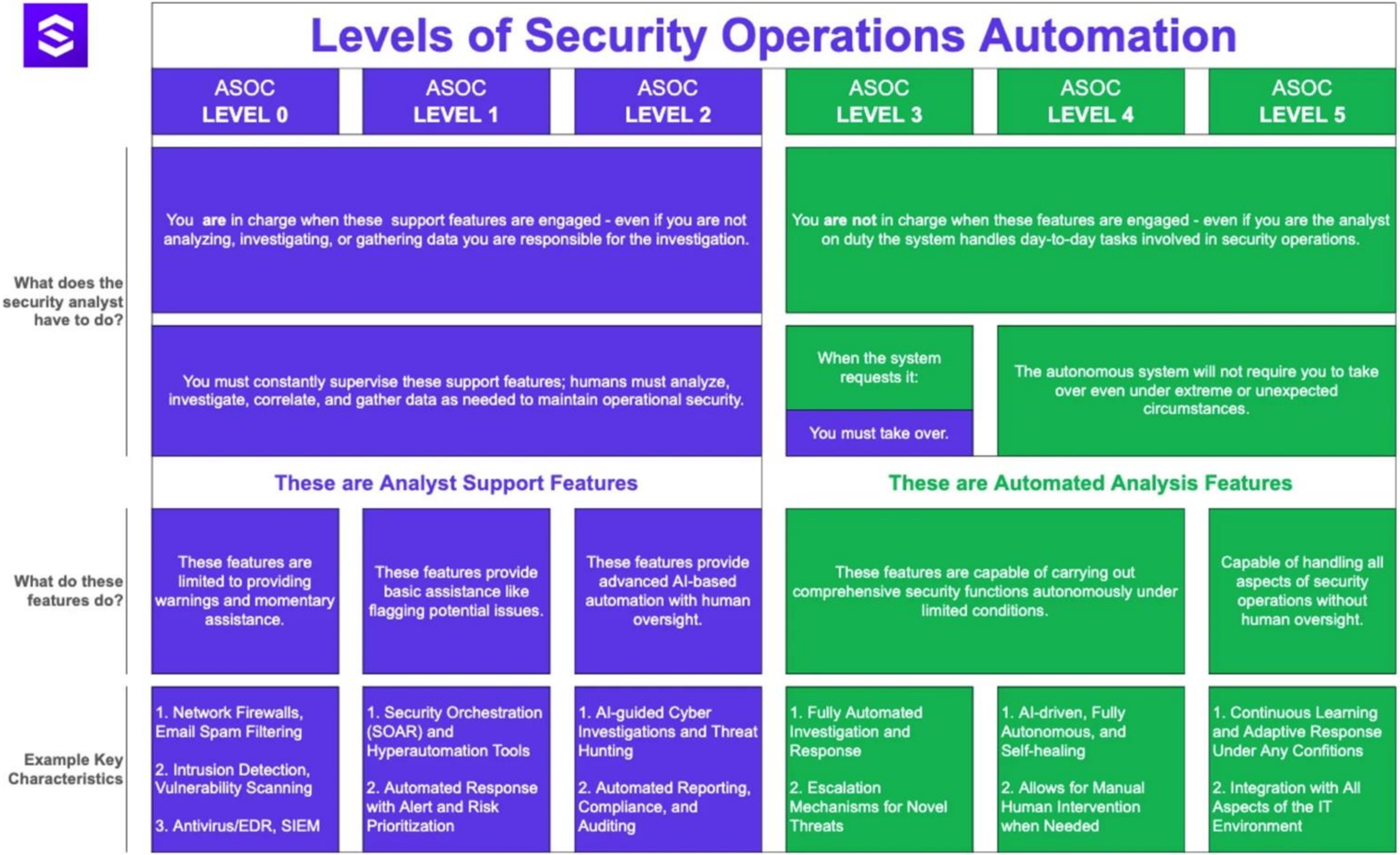
The system can autonomously detect, analyze, respond to, and mitigate threats in real-time, without needing human input.

Advanced AI Algorithms

Data models and data science techniques that continuously learn and adapt to new threats.

Automatic Recovery

Recover from any incident, including complex breaches, anomalous situations, and system failures.



Levels of Security Operations Automation

	ASOC LEVEL 0	ASOC LEVEL 1	ASOC LEVEL 2	ASOC LEVEL 3	ASOC LEVEL 4	ASOC LEVEL 5
What does the security analyst have to do?	You **are** in charge when these support features are engaged - even if you are not analyzing, investigating, or gathering data you are responsible for the investigation.			You **are not** in charge when these features are engaged - even if you are the analyst on duty the system handles day-to-day tasks involved in security operations.		
	You must constantly supervise these support features; humans must analyze, investigate, correlate, and gather data as needed to maintain operational security.			When the system requests it: You must take over.	The autonomous system will not require you to take over even under extreme or unexpected circumstances.	
	These are Analyst Support Features			These are Automated Analysis Features		
What do these features do?	These features are limited to providing warnings and momentary assistance.	These features provide basic assistance like flagging potential issues.	These features provide advanced AI-based automation with human oversight.	These features are capable of carrying out comprehensive security functions autonomously under limited conditions.		Capable of handling all aspects of security operations without human oversight.
Example Key Characteristics	1. Network Firewalls, Email Spam Filtering 2. Intrusion Detection, Vulnerability Scanning 3. Antivirus/EDR, SIEM	1. Security Orchestration (SOAR) and Hyperautomation Tools 2. Automated Response with Alert and Risk Prioritization	1. AI-guided Cyber Investigations and Threat Hunting 2. Automated Reporting, Compliance, and Auditing	1. Fully Automated Investigation and Response 2. Escalation Mechanisms for Novel Threats	1. AI-driven, Fully Autonomous, and Self-healing 2. Allows for Manual Human Intervention when Needed	1. Continuous Learning and Adaptive Response Under Any Confitions 2. Integration with All Aspects of the IT Environment

Leadership in the Era of AI

Executive Roles in the Era of AI

I'M THE CHIEF INFORMATION OFFICER YOU WISH YOU HAD

Upskilling & Adapting

Digital Transformation
Operational Efficiency
IT Infrastructure

++Strategic Technologies
++AI Business Integration

Accountability & Authority

Data Security & Integrity
Expanding CIA^3 Triad*
Risk Management

++Increased Efficiency
++Align with the Business

AI Strategic Leadership

Align AI with Business
AI Technology Oversight

Ethics & Governance
Regulatory Compliance
Advocacy & Education

The Future of Work is Ethical & Human

Successful Leaders Will Promote AI-Augmented Success While Navigating Uncertainties

Rethink Workflows

Integrate AI to optimize processes, enhance efficiency, maximize value, and transform operational dynamics.

Redefine Decision-Making

Adapt decision-making to the rapid pace of AI ensuring that decisions are informed by AI insights but driven by human judgment.

Inclusive AI Culture

Foster an inclusive AI culture incorporating diverse perspectives, leading to reduced biases and improved decision-making.

Seek to Understand

Stay informed to remain at the forefront of technological innovation and secure your relevance in an AI-driven future.

AI the Collaborator

Embrace AI as a collaborator, not a competitor, to enhance productivity, drive innovation, and position for success.

Think Globally

Adopt a global perspective to develop comprehensive strategies and maximize impact in an increasingly connected world.

Our Journey Towards Autonomous Security

Enabling security teams to do more with less

Disrupted market with AI Powered Protection

The most advanced AI security analyst

Autonomous AI security tools

Ransomware Protection with Automated Remediation

Leveraging AI-powered detections + Storyline technology to automatically kill and quarantine and rollback changes made by malicious actors.

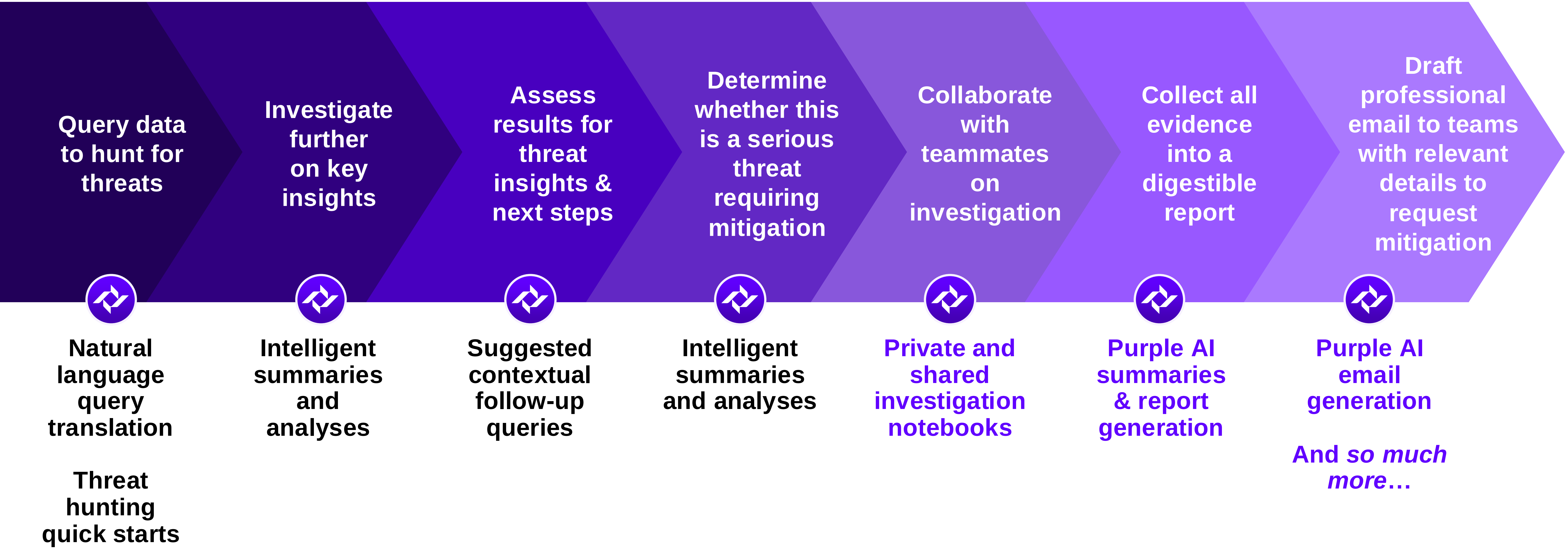
Purple AI: Accelerating Security Operations

Intelligent hunting, investigation, and support assistance powered by GenAI.

Purple AI: Autonomous Security

Auto-triage. Auto-investigations. Purple-powered Hyperautomation. Automate manual work.

We expanded our approach to meet today's SecOps investigation needs



Query data to hunt for threats

Natural language query translation

Threat hunting quick starts

Investigate further on key insights

Intelligent summaries and analyses

Assess results for threat insights & next steps

Suggested contextual follow-up queries

Determine whether this is a serious threat requiring mitigation

Intelligent summaries and analyses

Collaborate with teammates on investigation

Private and shared investigation notebooks

Collect all evidence into a digestible report

Purple AI summaries & report generation

Draft professional email to teams with relevant details to request mitigation

Purple AI email generation

And *so much more…*

SentinelOne

Key Takeaways

Data Science Techniques

Increasingly sophisticated and capable of handling the entire cybersecurity operation.

Levels of Autonomy

The appropriate level of autonomy will vary based on organizational needs and business objectives.

The Human Factor

Humans should continue to learn how to perform dynamic security tasks themselves.

Set New Benchmarks

AI will set new benchmarks in three key areas: Speed, Expertise, and Volume.

Deprecated SOC Tiers

The typical tiered SOC structure is changing and will soon become obsolete.

Strategic Focus

Security analysts will not be needed for day-to-day operations and can focus on higher-level tasks.

SentinelOne
Secure Tomorrow

Thank You

Sentinelone.com