Intrusion Detection System Manager (IdsM)

AUTOSAR Standard Module Introduction

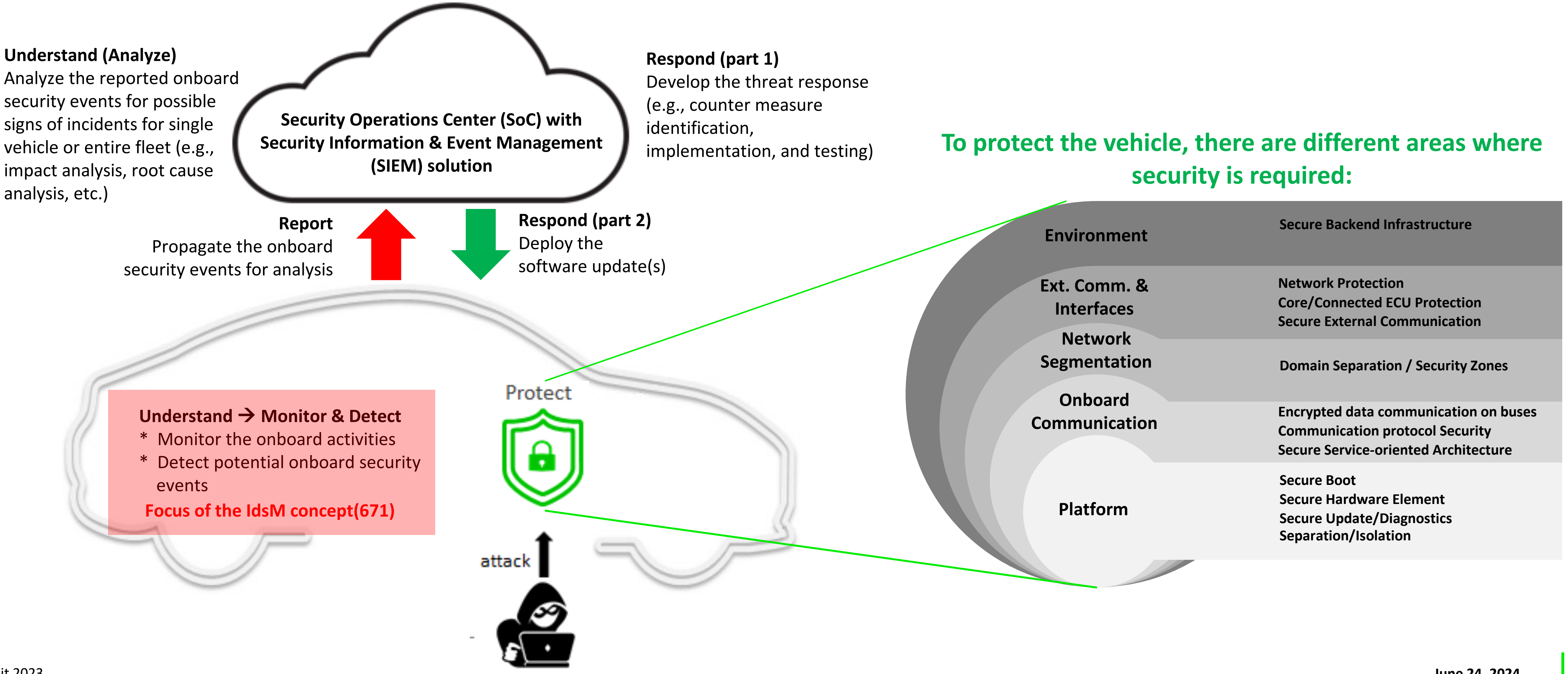
Aaron Galbraith, Pre-Sales Engineer

Lucian Iliescu, Software Architect

Intrusion Detection System Manager (IdsM)

Target of AUTOSAR Standard “Intrusion Detection System Manager (671)”

- Intrusion Detection System (IDS) is intended to protect the vehicle from unwanted intrusion and can be realized by an IdsM through the process of: **Protect → Understand** (Monitoring & Detection) **→ Report → Understand** (Analysis) **→ Respond**



Understand (Analyze)
Analyze the reported onboard security events for possible signs of incidents for single vehicle or entire fleet (e.g., impact analysis, root cause analysis, etc.)

Security Operations Center (SoC) with Security Information & Event Management (SIEM) solution

Respond (part 1)
Develop the threat response (e.g., counter measure identification, implementation, and testing)

Report
Propagate the onboard security events for analysis

Respond (part 2)
Deploy the software update(s)

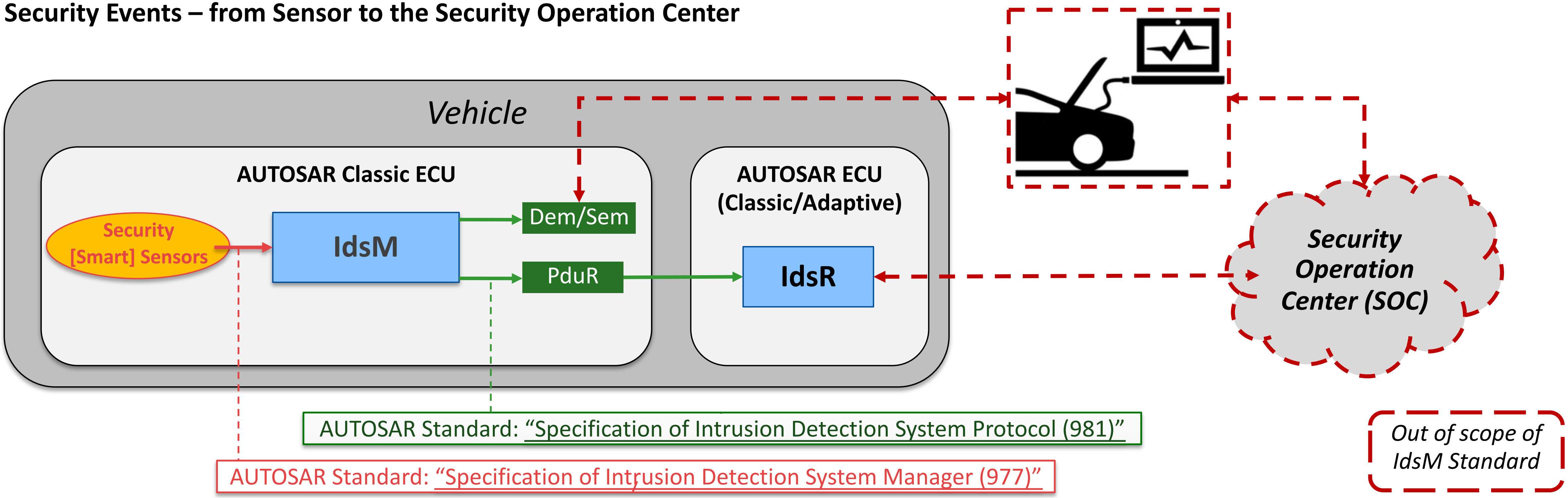
Understand → Monitor & Detect
* Monitor the onboard activities
* Detect potential onboard security events
Focus of the IdsM concept(671)

To protect the vehicle, there are different areas where security is required:

Environment	Secure Backend Infrastructure
Ext. Comm. & Interfaces	Network Protection Core/Connected ECU Protection Secure External Communication
Network Segmentation	Domain Separation / Security Zones
Onboard Communication	Encrypted data communication on buses Communication protocol Security Secure Service-oriented Architecture
Platform	Secure Boot Secure Hardware Element Secure Update/Diagnostics Separation/Isolation

Intrusion Detection System Manager (IdsM)

Security Events – from Sensor to the Security Operation Center


Vehicle
AUTOSAR Classic ECU
Security [Smart] Sensors
IdsM
Dem/Sem
PduR
AUTOSAR ECU (Classic/Adaptive)
IdsR
Security Operation Center (SOC)
AUTOSAR Standard: "Specification of Intrusion Detection System Protocol (981)"
AUTOSAR Standard: "Specification of Intrusion Detection System Manager (977)"
Out of scope of IdsM Standard

RECAP:

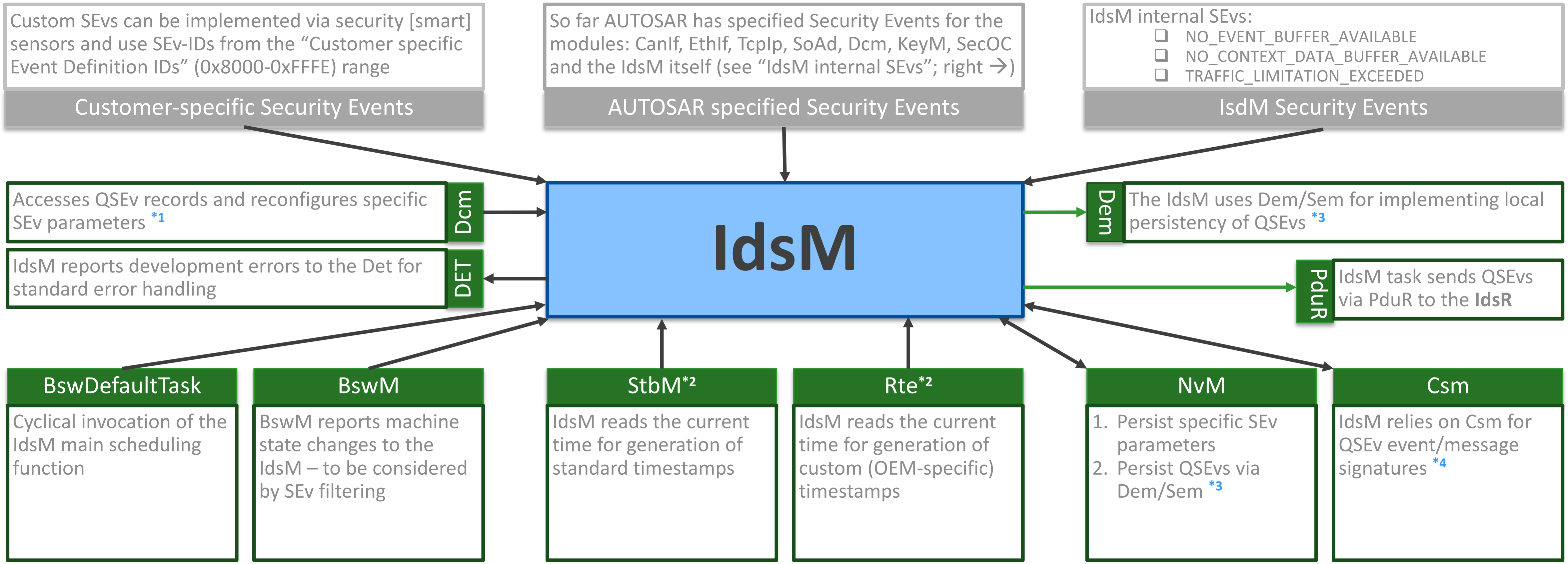
- ❑ One IdsM per ECU, one IsdR per vehicle, one SOC per OEM/product line
- ❑ **Smart Sensors** might collect and assess multiple events before reporting

Some more AUTOSAR specifications for IDSM:

- ❑ "Intrusion Detection System Manager (671)"
- ❑ "Requirements on Intrusion Detection System (976)"
- ❑ "Specification of Intrusion Detection System Manager for Adaptive Platform (978)"
- ❑ "Security Extract Template (820)"

Intrusion Detection System Manager (IdsM)

Interfacing with other Modules



Custom SEvs can be implemented via security [smart] sensors and use SEv-IDs from the “Customer specific Event Definition IDs” (0x8000-0xFFFE) range

Customer-specific Security Events

So far AUTOSAR has specified Security Events for the modules: CanIf, EthIf, TcpIp, SoAd, Dcm, KeyM, SecOC and the IdsM itself (see “IdsM internal SEvs”; right →)

AUTOSAR specified Security Events

IdsM internal SEvs:

- ❑ NO_EVENT_BUFFER_AVAILABLE
- ❑ NO_CONTEXT_DATA_BUFFER_AVAILABLE
- ❑ TRAFFIC_LIMITATION_EXCEEDED

IsdM Security Events

Dcm: Accesses QSEv records and reconfigures specific SEv parameters *1

DET: IdsM reports development errors to the Det for standard error handling

IdsM

Dem: The IdsM uses Dem/Sem for implementing local persistency of QSEvs *3

PduR: IdsM task sends QSEvs via PduR to the **IdsR**

BswDefaultTask: Cyclical invocation of the IdsM main scheduling function

BswM: BswM reports machine state changes to the IdsM – to be considered by SEv filtering

StbM*2: IdsM reads the current time for generation of standard timestamps

Rte*2: IdsM reads the current time for generation of custom (OEM-specific) timestamps

NvM:

1. Persist specific SEv parameters
2. Persist QSEvs via Dem/Sem *3

Csm: IdsM relies on Csm for QSEv event/message signatures *4

*1 Support of reading/changing the reporting mode is OPTIONAL

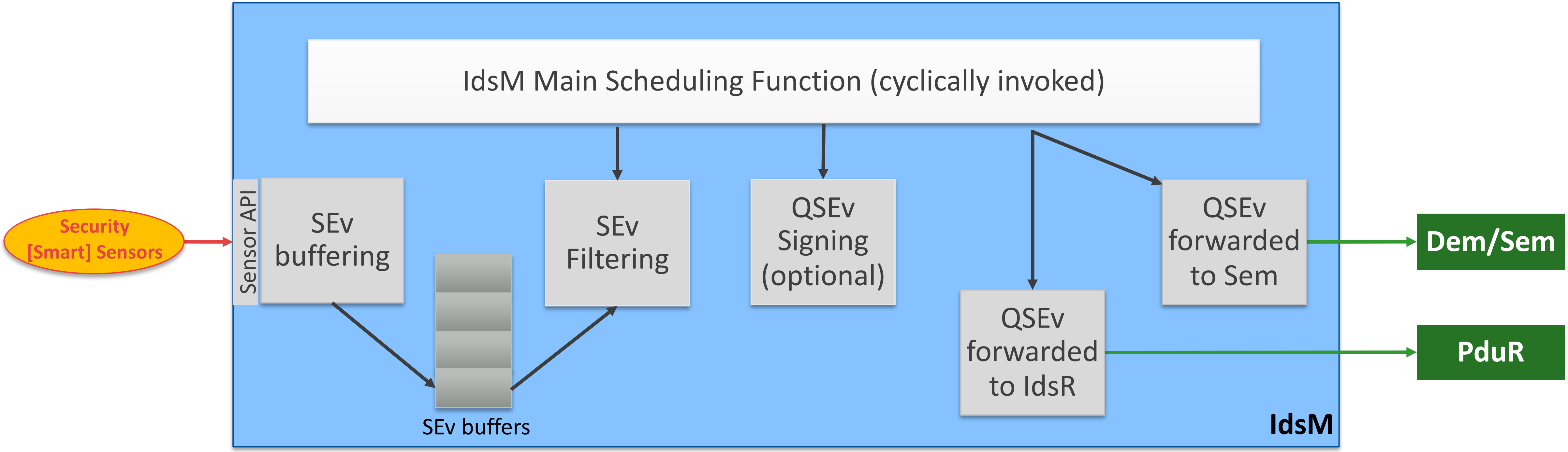
*2 Generation of timestamps for QSEvs is OPTIONAL

*3 Storing QSEvs persistent on-board via Sem & NvM is OPTIONAL

*4 Protecting QSEvs by adding a signature is OPTIONAL

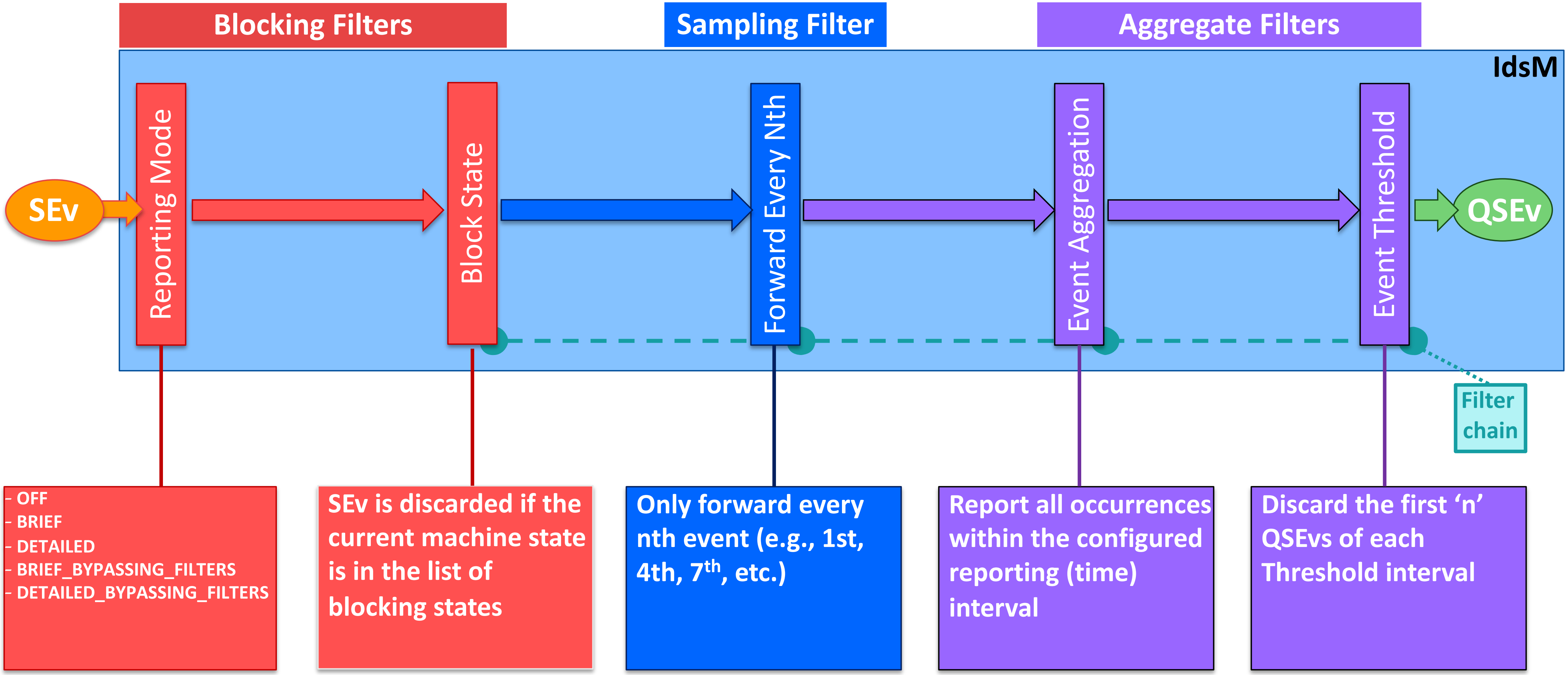
Intrusion Detection System Manager (IdsM)

Processing/Qualifying Security Events (SEv)



Intrusion Detection System Manager (IdsM)

Security Event (SEv) Filtering



Blocking Filters

Sampling Filter

Aggregate Filters

IdsM

SEv

Reporting Mode

Block State

Forward Every Nth

Event Aggregation

Event Threshold

QSEv

Filter chain

- OFF
- BRIEF
- DETAILED
- BRIEF_BYPASSING_FILTERS
- DETAILED_BYPASSING_FILTERS

SEv is discarded if the current machine state is in the list of blocking states

Only forward every nth event (e.g., 1st, 4th, 7th, etc.)

Report all occurrences within the configured reporting (time) interval

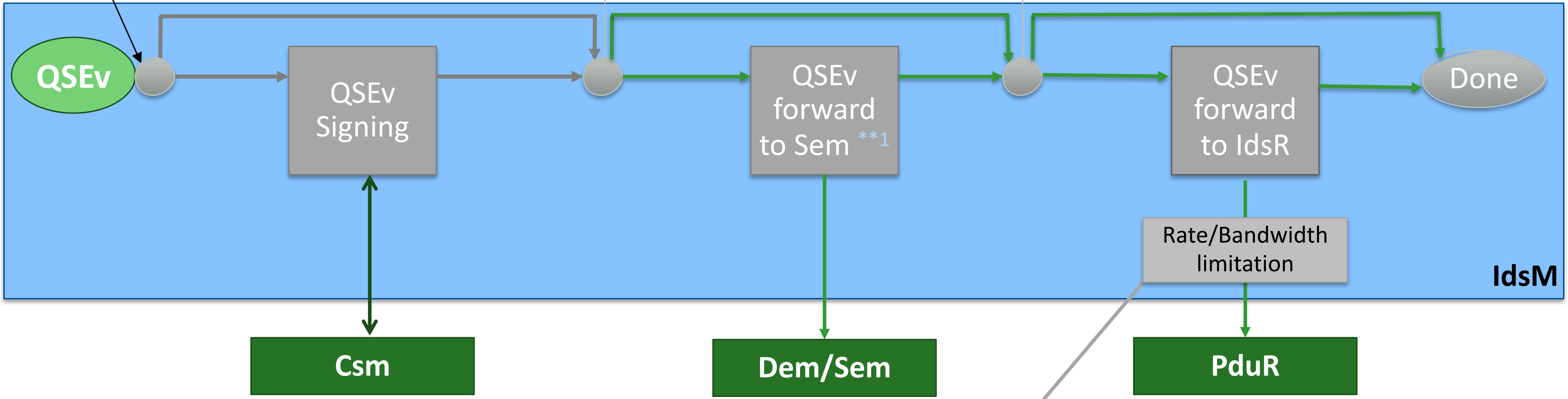
Discard the first ‘n’ QSEvs of each Threshold interval

Intrusion Detection System Manager (IdsM)

Qualified Security Event (QSEv) Signing and Reporting

QSEv Signing: this configuration is not QSEv-specific, but applies to all QSEvs handled by the IdsM instance

QSEv Sink/s: QSEv specific configuration



Rate limitation:

number of QSEvs per time interval

Bandwidth limitation :

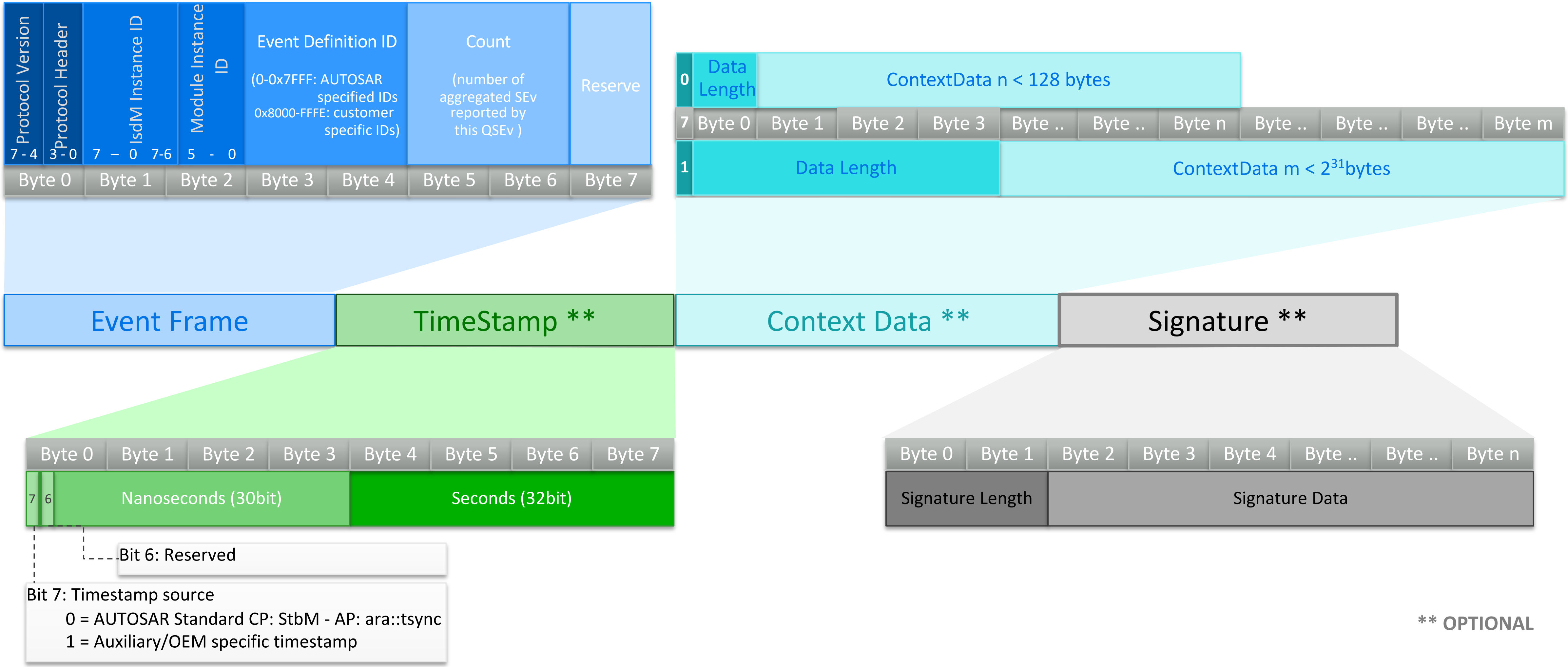
Number of bytes per time interval

NOTE. This filter is not QSEv specific but applies to all QSEvs handled by the IdsM instance.

*[**1] Local persistency is still in DRAFT in “Specification of Intrusion Detection System Manager (977)”*

Intrusion Detection System Manager (IdsM)

IDS event format (QSEv format)



Protocol Version 7 - 4

Protocol Header 3 - 0

IsdM Instance ID 7 – 0 7-6

Module Instance ID 5 - 0

Event Definition ID

(0-0x7FFF: AUTOSAR specified IDs
0x8000-FFFE: customer specific IDs)

Count

(number of aggregated SEv reported by this QSEv)

Reserve

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7

0 | Data Length | ContextData n < 128 bytes

7 | Byte 0 | Byte 1 | Byte 2 | Byte 3 | Byte .. | Byte .. | Byte n | Byte .. | Byte .. | Byte .. | Byte m

1 | Data Length | ContextData m < 2^{31}bytes

Event Frame	TimeStamp **	Context Data **	Signature **

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7

7 | 6 | Nanoseconds (30bit) | Seconds (32bit)

Bit 6: Reserved

Bit 7: Timestamp source
0 = AUTOSAR Standard CP: StbM - AP: ara::tsync
1 = Auxiliary/OEM specific timestamp

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte ..	Byte ..	Byte n

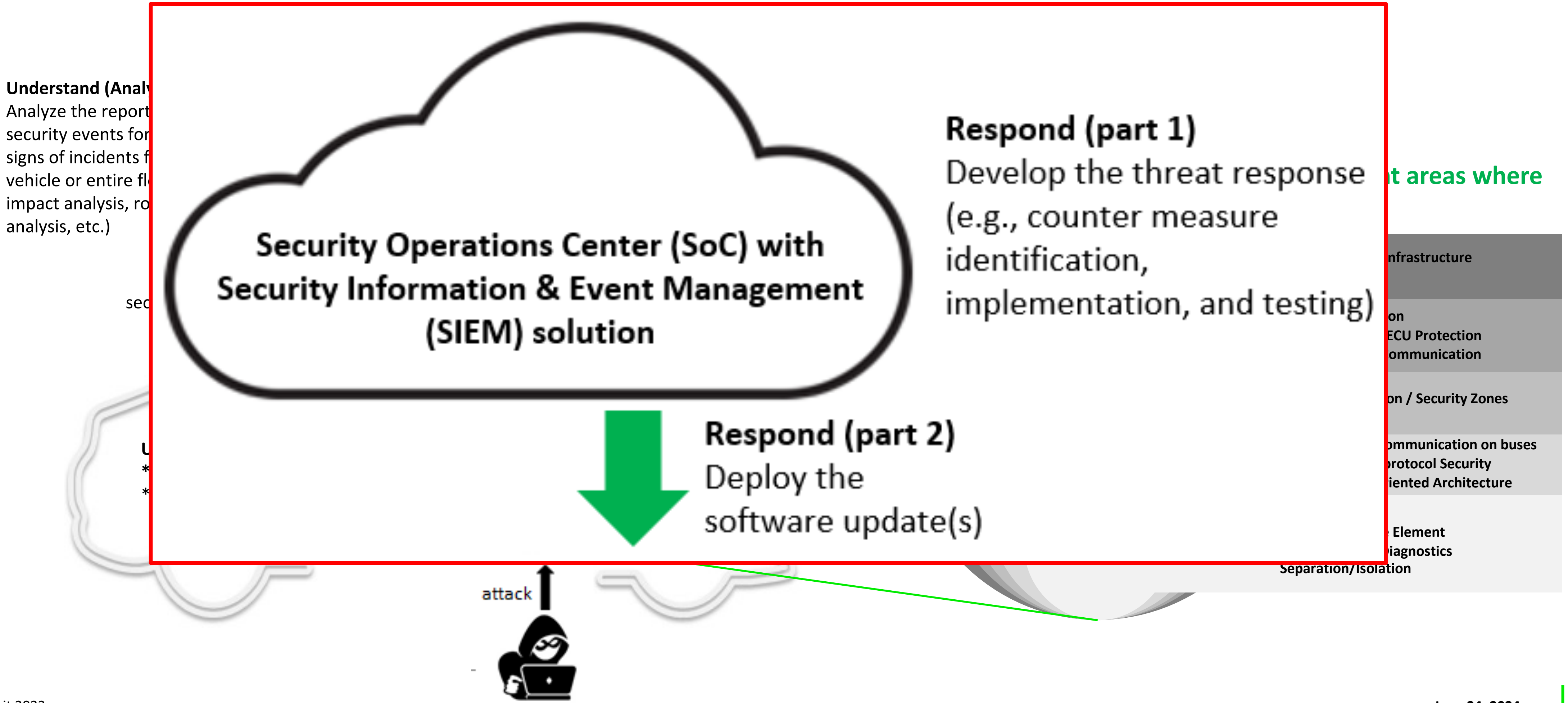
Signature Length | Signature Data

** OPTIONAL

Intrusion Detection System Manager (IdsM)

Current Limitation/Vulnerability of Ids Systems

Protect → **Understand** (Monitoring & Detection) → **Report** → **Understand** (Analysis) → **Respond**



Understand (Analy
Analyze the report
security events for
signs of incidents f
vehicle or entire fl
impact analysis, ro
analysis, etc.)

Security Operations Center (SoC) with Security Information & Event Management (SIEM) solution

Respond (part 1)
Develop the threat response (e.g., counter measure identification, implementation, and testing)

Respond (part 2)
Deploy the software update(s)

Thank you