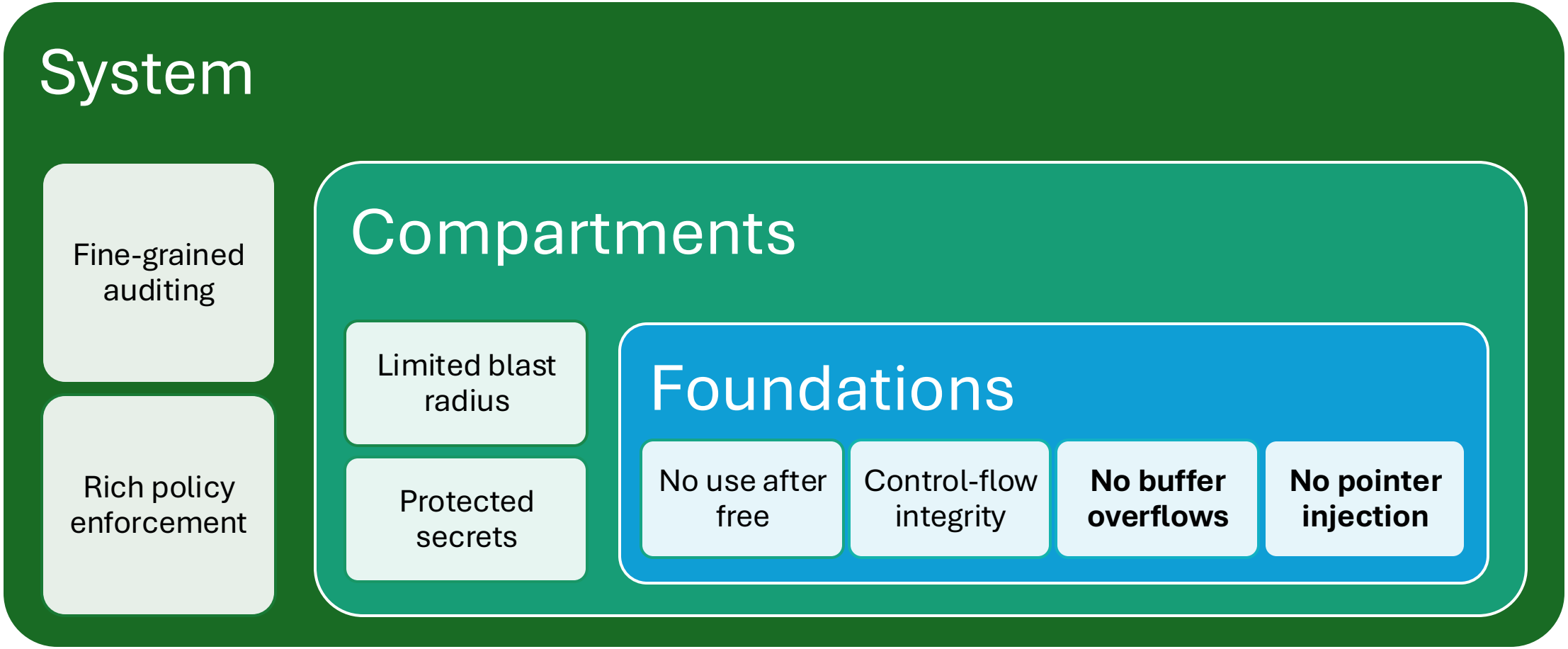
CHERIoT Audit

David Chisnall

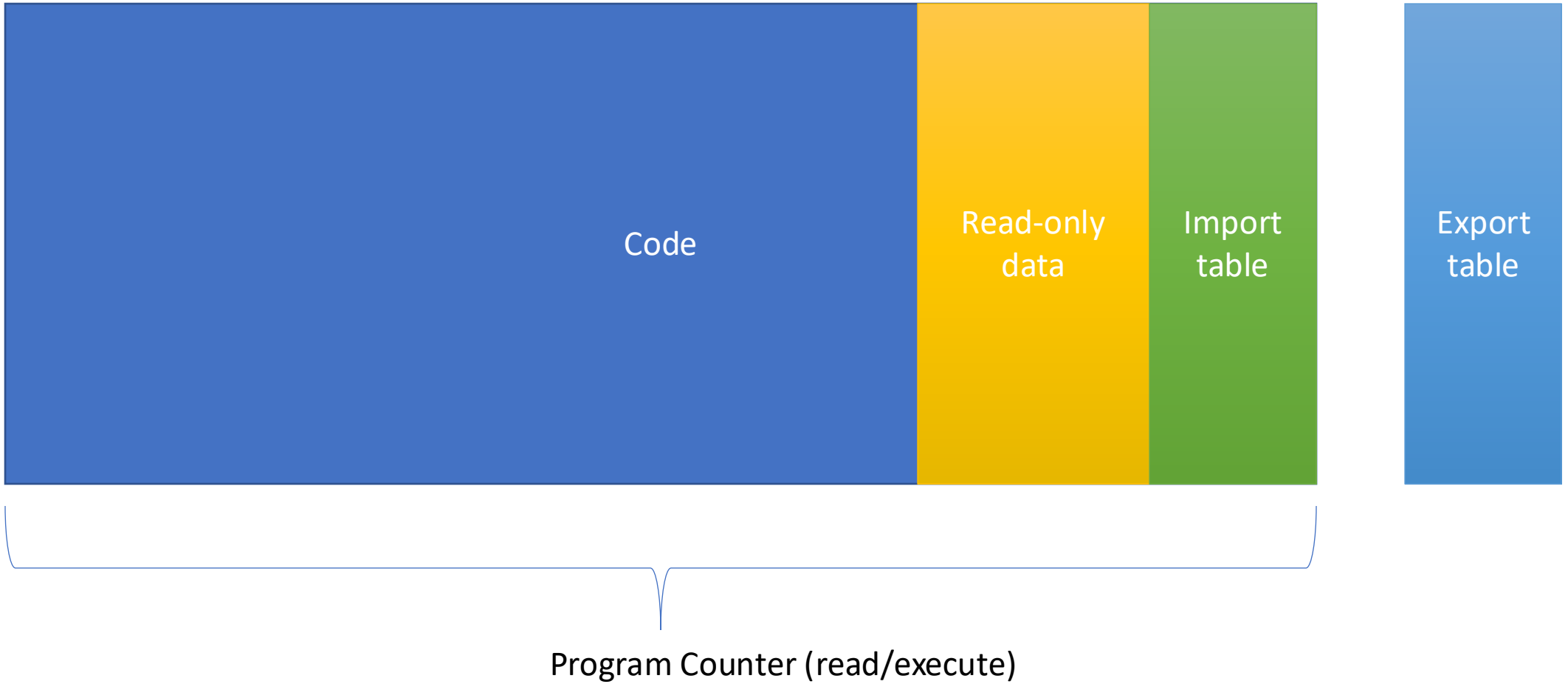

Memory safety is a building block

CHERIoT provides layered security

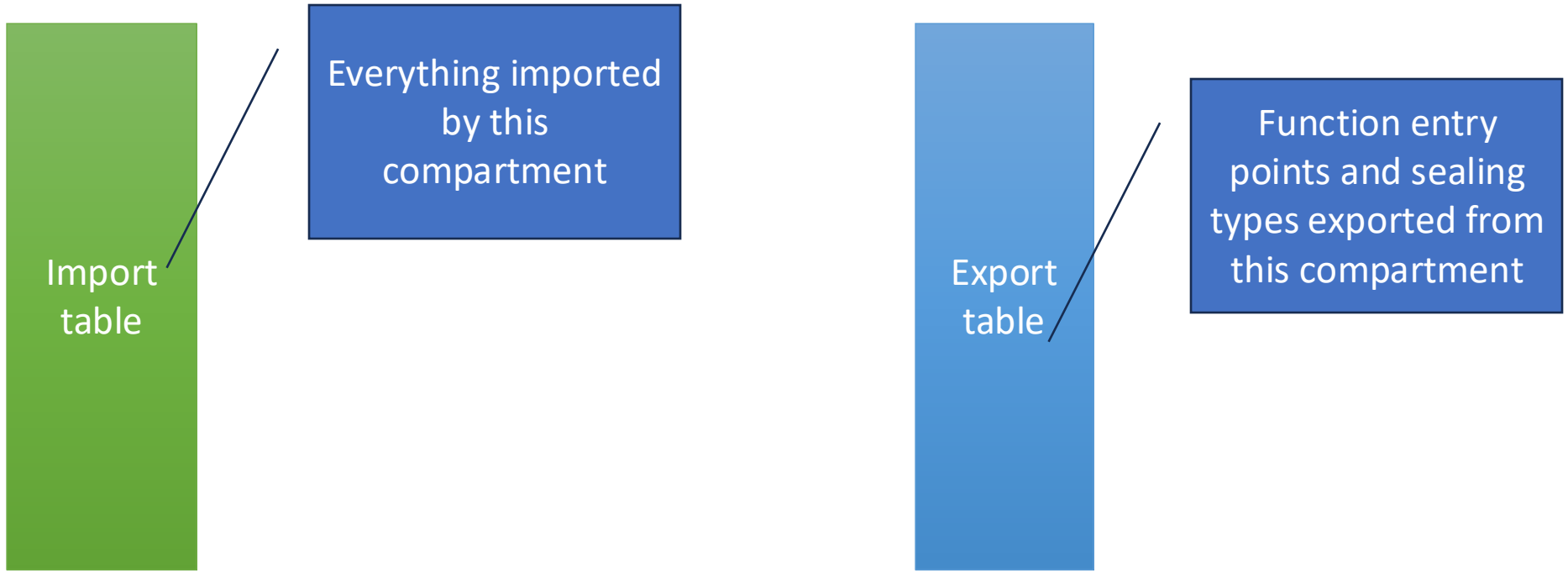


Compartments are code and data

Compartments are code and data and exports



Compartment graphs are imports and exports



There are many kinds of import!

- Static sealed objects
- Shared objects
- Functions
  - From shared libraries or compartments
  - With interrupts enabled or disabled
- Sealing keys

The linker generates detailed JSON for exports

```
{
  "export_symbol":
"__export.sealing_type.alloc.MallocKey",
  "exported": true,
  "kind": "SealingKey"
},
```

The linker generates detailed JSON for exports


```
{
  "export_symbol":
"__export_alloc__Z20heap_quota_remainingP10SObjStruc
t",
  "exported": true,
  "interrupt_status": "enabled",
  "kind": "Function",
  "register_arguments": 1,
  "start_offset": 192
},
```

The linker generates detailed JSON for imports


```
{
  "kind": "SharedObject",
  "length": 4,
  "permits_load": true,
  "permits_load_mutable": true,
  "permits_load_store_capabilities": true,
  "permits_store": true,
  "shared_object": "allocator_epoch",
  "start": 2147604608
}
```

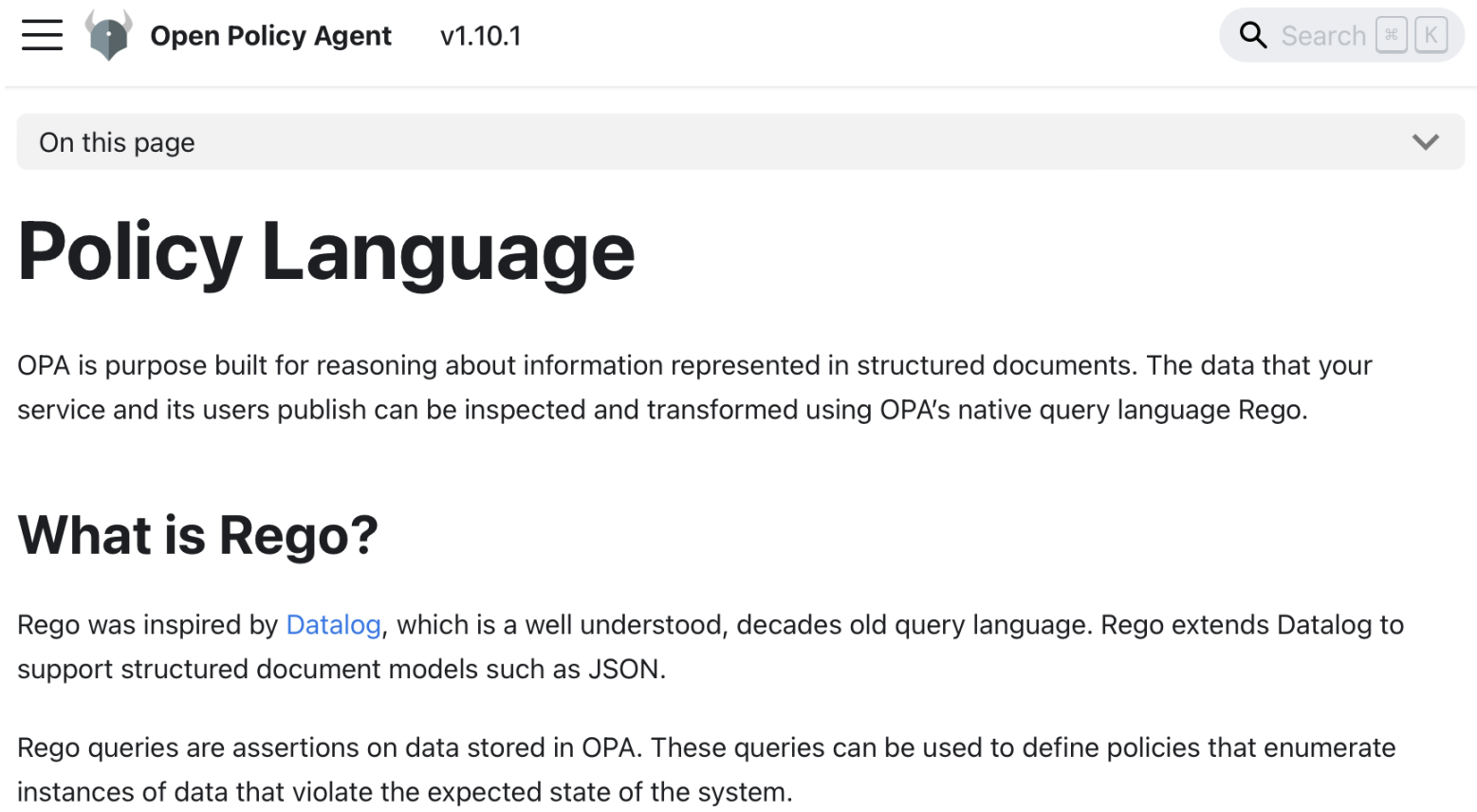
The linker generates detailed JSON for imports


```
{
  "kind": "MMIO",
  "length": 4096,
  "permits_load": true,
  "permits_load_mutable": false,
  "permits_load_store_capabilities": false,
  "permits_store": true,
  "start": 2197815296
}
```

The linker generates detailed JSON for imports


```
{
  "contents": "00040000 00000000 00000000 00000000 00000000
00000000",
  "kind": "SealedObject",
  "sealing_type": {
    "compartment": "alloc",
    "key": "MallocKey",
    "provided_by":
"build/cheriot/cheriot/release/cheriot.allocator.compartment"
,
    "symbol": "__export.sealing_type.alloc.MallocKey"
  }
}
```

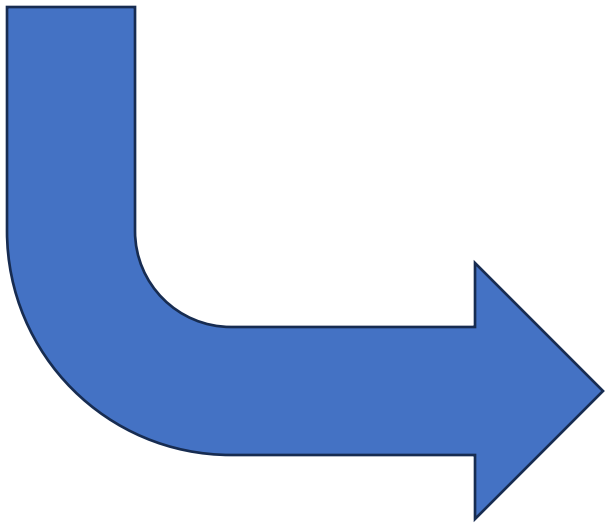
CHERIoT Audit uses Rego



Rego can inspect firmware

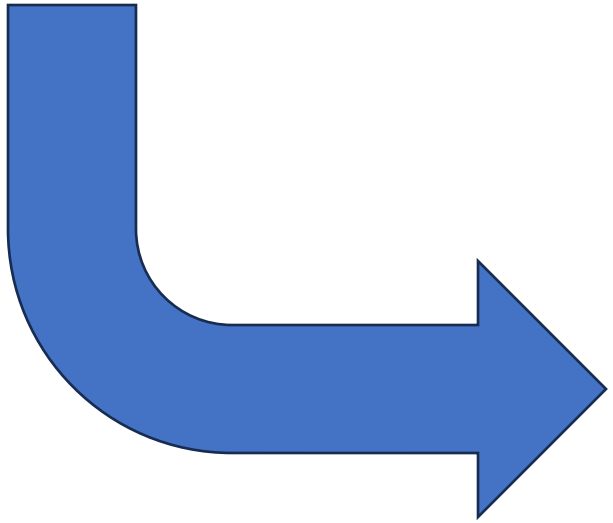
How much memory are all compartments allowed to allocate, between them?

```
sum([
data.rtos.decode_allocator_capability(c).quota |
c = input.compartments[_].imports[_] ;
data.rtos.is_allocator_capability(c) ])
```



```
1078272
```

`data.network_stack.all_connection_capabilities`

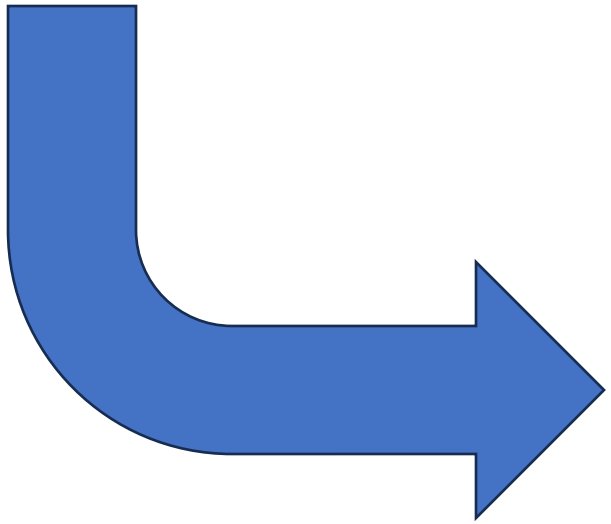


```
[
  {
    "capability": {
      "connection_type": "UDP",
      "host": "pool.ntp.org",
      "port": 123
    },
    "owner": "SNTP"
  },
  {
    "capability": {
      "connection_type": "TCP",
      "host": "example.com",
      "port": 443
    },
    "owner": "https_example"
  }
]
```

Which compartments can connect to which servers?

Which compartments can send TCP data?

```
data.compartment.compartments_calling_export_matching("TCPIP",
`network_socket_send\(.*`)
```



```
[
  "TLS"
]
```

Rego can enforce policies

Only the TLS stack may send TCP data

```
data.compartment.compartment_call_allow_list(
    "TCPIP",
    `network_socket_send\(.*`,
    {"TLS"})
```

Only the scheduler may access the CLINT

```
data.compartment.mmio_allow_list(
     "clint",
     {"scheduler"})
```

Only the SNTP compartment has write access to the published time result

```
data.compartment
    .shared_object_writeable_allow_list(
        "sntp_time_at_last_sync", {"SNTP"})
```

CHERIoT Audit enables fearless code reuse through end-to-end security design