A Practical Guide to Cyber Security Maturity

With Ben Marrable (Senior Security Strategist)

Ben Marrable,

Senior Security Strategist (CISSP) at **Somerford Associates**

About Me

- Dealt with Splunk technology for multiple years with Somerford
- Proficient expertise across the entire Splunk Security Suite
- Former UK National Champion of Ultimate Frisbee

Agenda

- Brief Introduction to Maturity Modelling
- The Splunk Security Data Journey
- Where to Start your Cyber Security journey
- How to progress your Cyber Security journey
- Key Topics
  - Data Models & CIM
  - Assets and Identities
  - RBA
  - Use Case Management
- Optimising your SOC

The Capability Maturing Model

Development Model created in 1986

Taking Processes from ad-hoc practice, right through to active optimisation

Level 1	Level 2	Level 3	Level 4	Level 5
Initial	**Repeatable**	**Defined**	**Managed**	**Optimising**
Processes are disorganised.	Processes are defined and documented.	Processes are standardised.	Processes are monitored and controlled.	Processes are continuously improved.

Security Maturity?

Many Differing Versions sharing the same principle:-

> **A Mapping of an Organisation's Security Posture in relation to the Business Requirements**

Understanding one's level of cyber security maturity allows for better understanding of the cyber **risks** facing the business. Aligning to an established model provides a prescriptive path to **further maturity** and **enhanced security** practice

Where to Start? - Repeatable

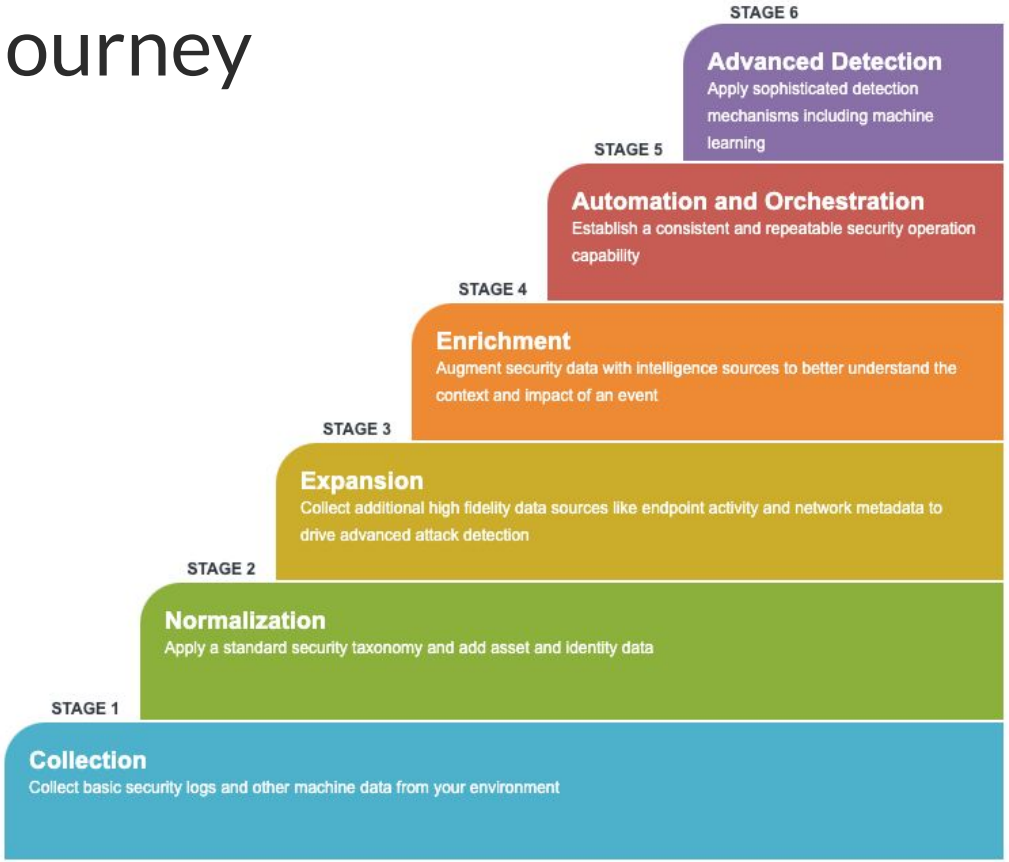
Key Priorities:

- Identify what your goals are
- Develop a Strategy on how to achieve those goals
- Establish repeatable processes to realise them
    - Logging and Monitoring
    - Security Awareness
    - Single Sign On
    - etc.

Splunk Security Data Journey

A 6 stage process to increase security maturity

Focused on data collection and extracting value from the data



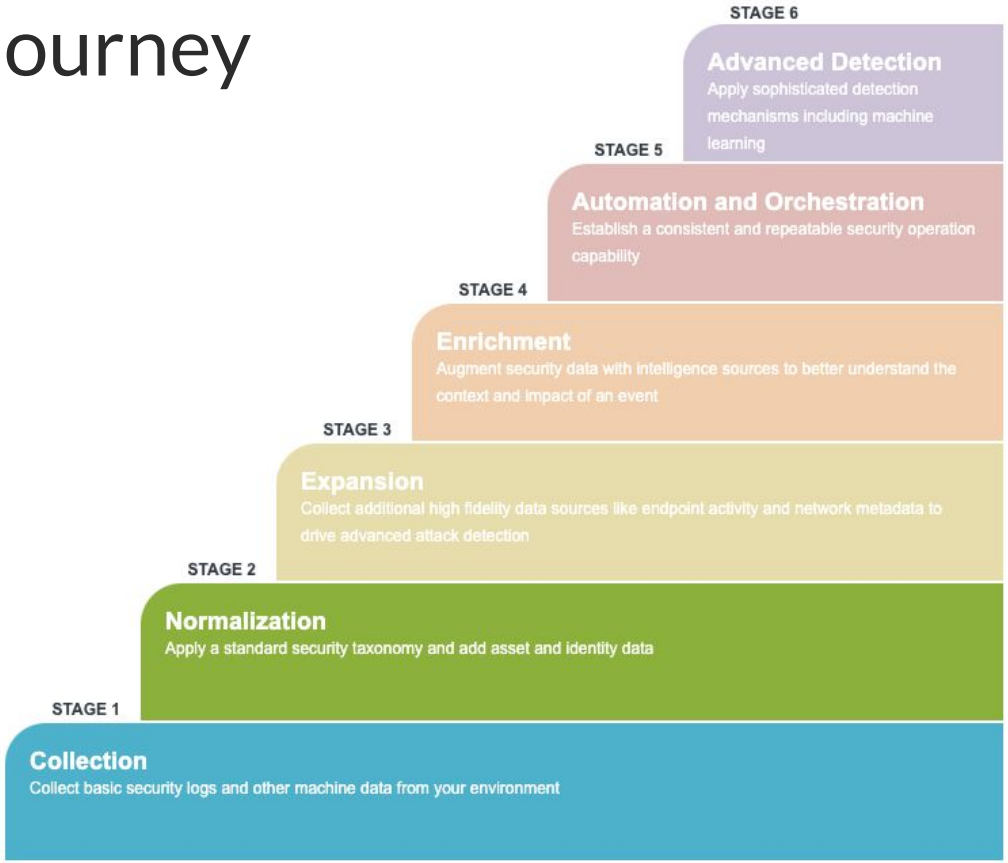
Splunk Security Data Journey

Establish the right baselines:-

Focus on **collecting** the right data into a central logging and monitoring platform.

Make the process repeatable:-

Normalising the data helps to streamline investigations and improve the effectiveness of your security team



What is a Data Model?

- A data model is an **abstraction** layer over the top of existing data or searches.
- Data models most commonly employed for **normalisation** and **acceleration**
- The model definition may contain a hierarchy, subdividing events into separate classes, similar to eventtypes

The Common Information Model (CIM)

- A collection of data models
  - To support the consistent normalized treatment of data
  - Delivers maximum efficiency at search time
- Datamodels - (Authentication, Change, Email, Malware, Network Resolution (DNS), Network Traffic, Updates, Vulnerabilities among others)
- Technology Add-Ons (TA's)

How to Progress? - Defined & Managed

We've established Repeatable practice, now to move onto Defined/Measured and Manageable

Key Priorities:

- Record and Track Meaningful Metrics
  - Mean Time to Respond
  - Mean Time to Resolve
  - Any and all relevant and controllable
- Processes in place to refine and reform secops in order to Reduce these key metrics wherever possible

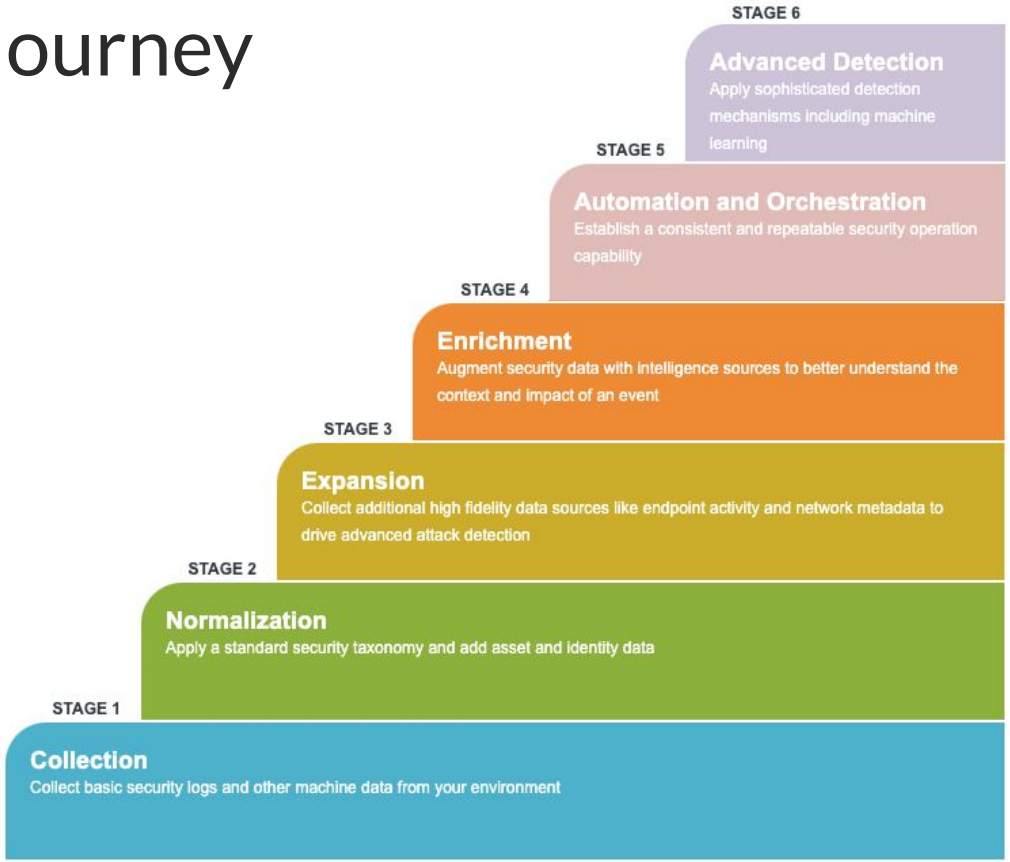
Splunk Security Data Journey

Define and measure metrics:-

Expand on the data coverage to utilise other technologies with the goal of reducing your mean time to respond.

Enhance your security alerts:-

Enrich the information presented to analysts to reduce your mean time to resolve



Assets and Identities

- CIS Controls
- Context
- Correlation

The Vital Questions

What is the Method of Collection?

How often do we poll the data?

How do we prioritise them?

How can we categorise them?

How can we identify the locations of resources?

Use Cases

- Define
- Structure
- Schedule
- Test

Use Case Management - Where to Start

“A use case is a security monitoring scenario that is aimed at the detection of manifestations of a cyber threat”

- Start with a Use Case Register
- Plan Future Growth Strategy - Don’t just implement use cases with little grounding
- Set up a testing plan

Use Case Management

Use a proven Framework - MaGMa

1. **Business Layer (Strategic)**

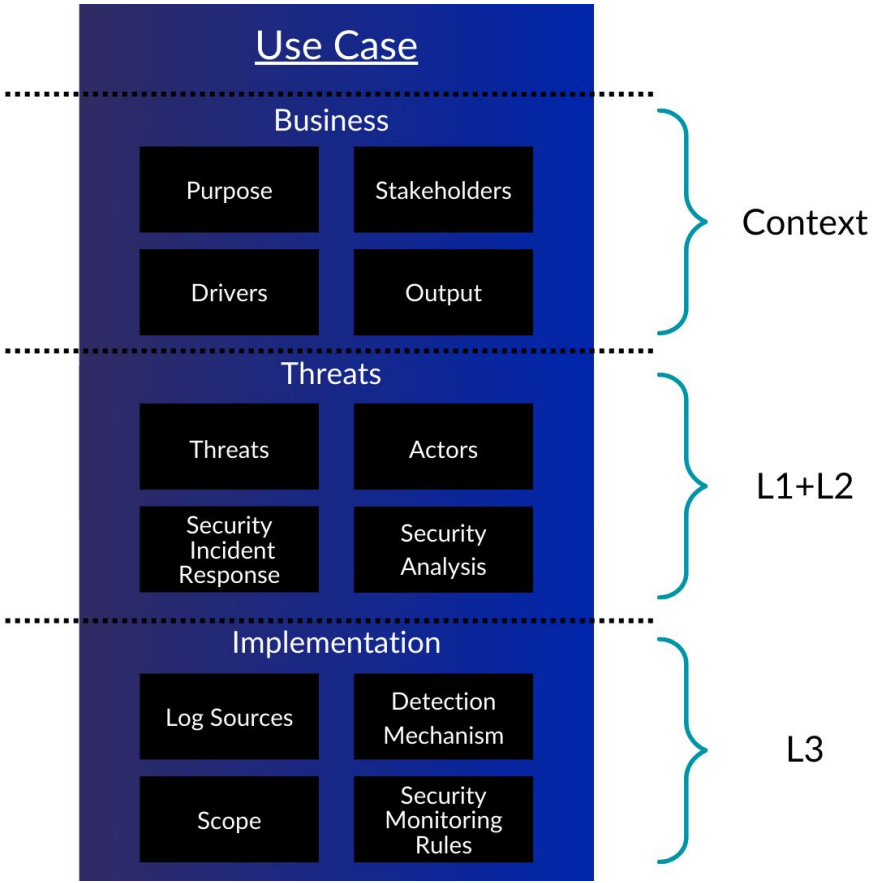
Defines how is the use case is connected to the organizations needs

2. **Threat Layer (Tactical)**

Defines the threat that the use cases are intended to detect

3. **Implementation Layer (Operational)**

Defines what aspects that are relevant for the implementation of the use case



Risk Based Alerting (RBA)

- What is Risk Based Alerting
- Why is it the future of SOC operations and detections
- The foundations for RBA with ES

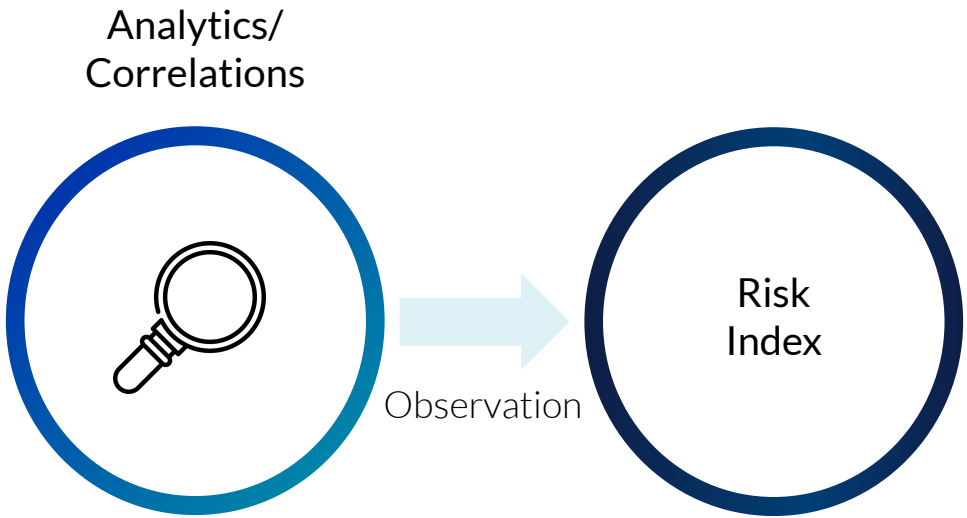
Alert Volumes Are Overwhelming SOCs

Over 40% of orgs receive 10,000+ alerts per day; experience 50%+ false positives

- Abandoned alerts
- Suppressed alerts
- Slow detection / response
- Analyst burnout

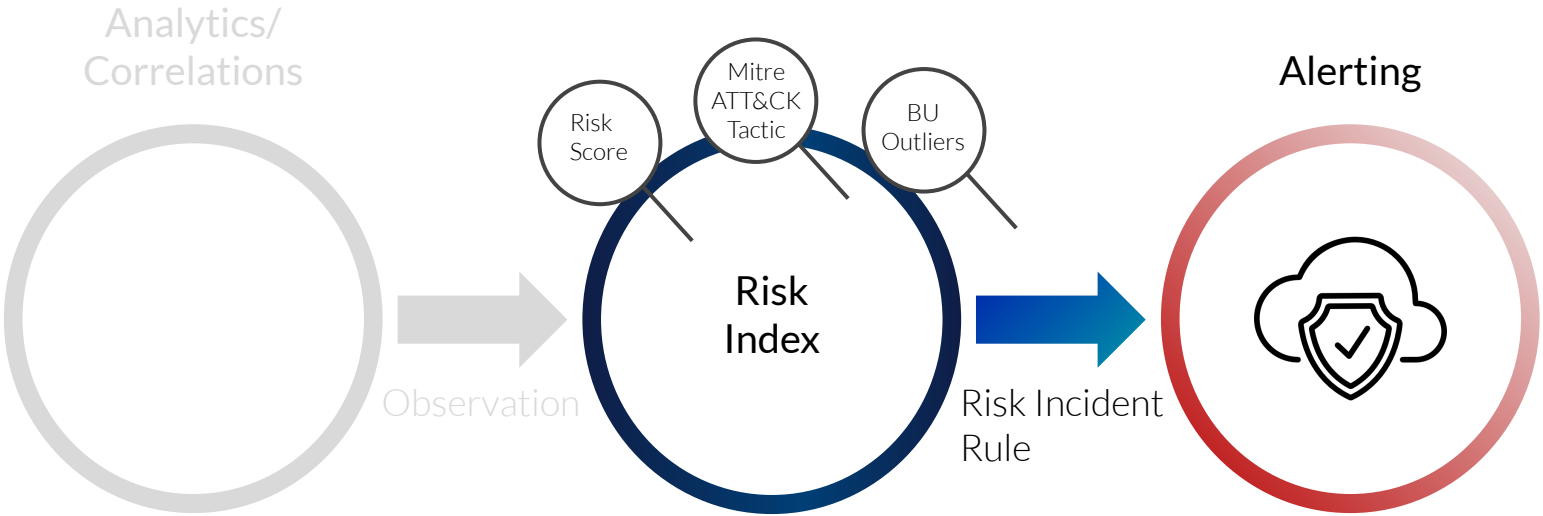
Risk-Based Alerting to the Rescue

Dramatically reduce alert volumes while improving your security posture



Risk-Based Alerting to the Rescue

Dramatically reduce alert volumes while improving your security posture



Multiple Events

Using Risk Based Alerting

9:55am

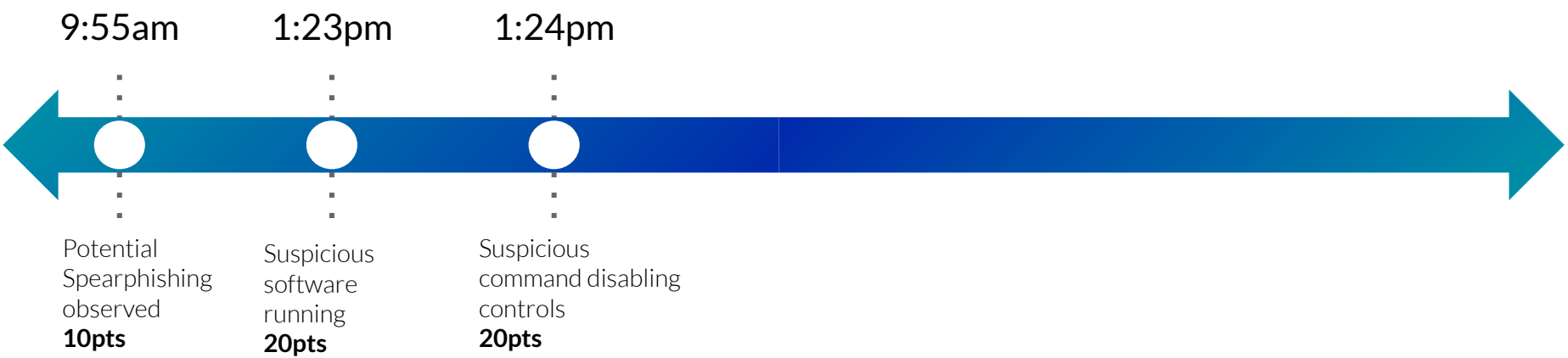
Potential Spearphishing observed
10pts

Multiple Events

Using Risk Based Alerting

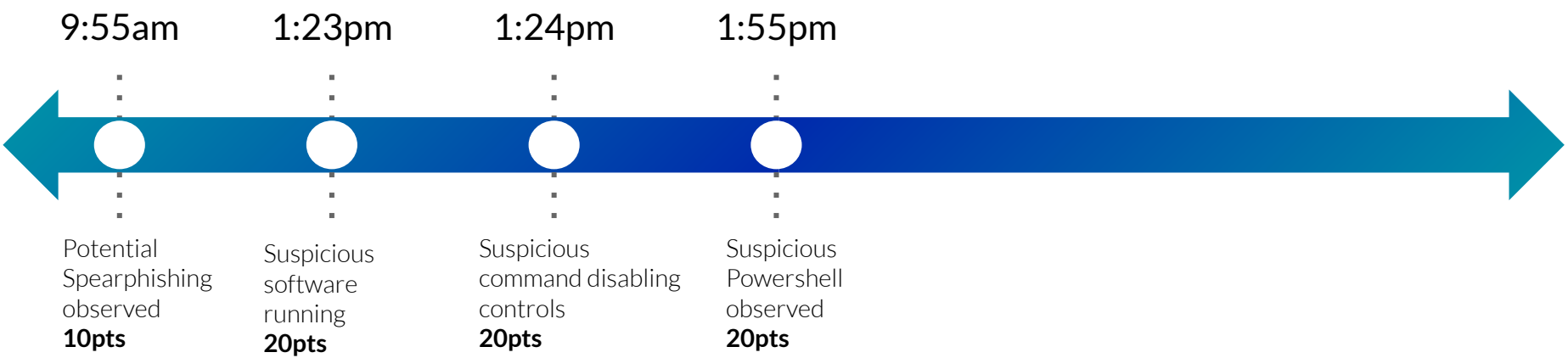
Multiple Events

Using Risk Based Alerting



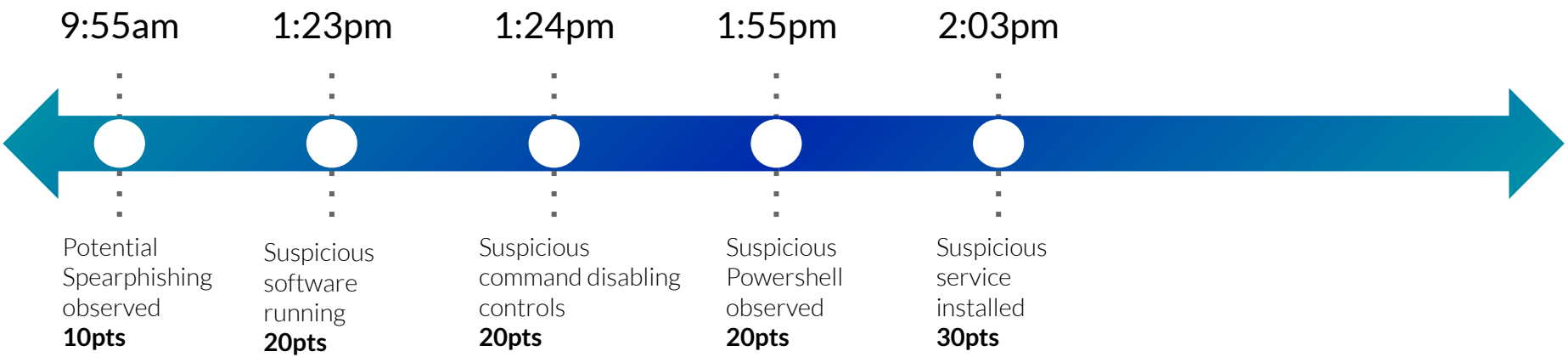
Multiple Events

Using Risk Based Alerting



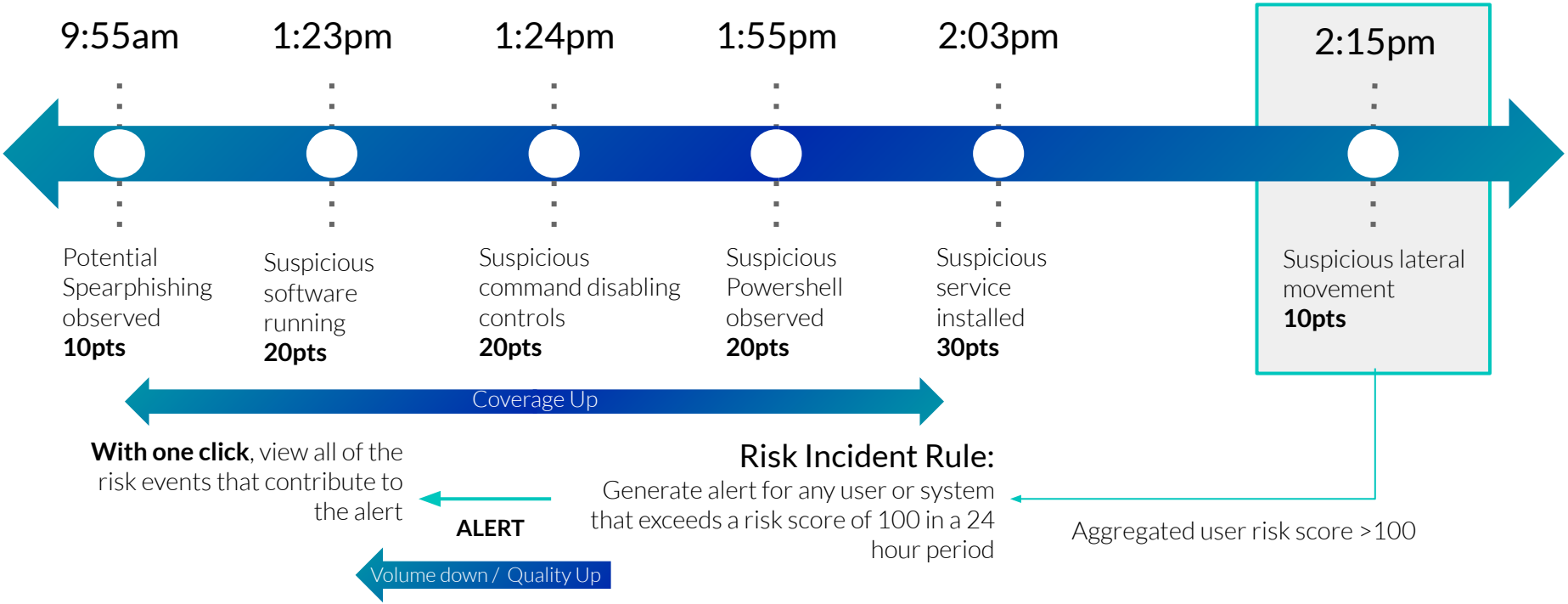
Multiple Events

Using Risk Based Alerting



Multiple Events

Using Risk Based Alerting



The Foundations for RBA

Asset and Identity Framework

Risk Rules and their risk scores with

- ➔ An **Impact** Level
- ➔ A **Confidence** Percentage
- ➔ MITRE Tactic & Technique, Cyber Kill Chain phase, other **Annotations**
- ➔ A detailed **Risk Message**

Risk Indicator Rules

Risk Factors

How to Progress? - Optimising

We've established a Repeatable, Defined and Manageable security operations practice by now. Time to optimise that

Key Priorities:

- Automate Repetitive Tasks
- Orchestrate Security Tooling to simplify response processes
- Continually look to reduce the key metrics
- Implement Advanced Detections

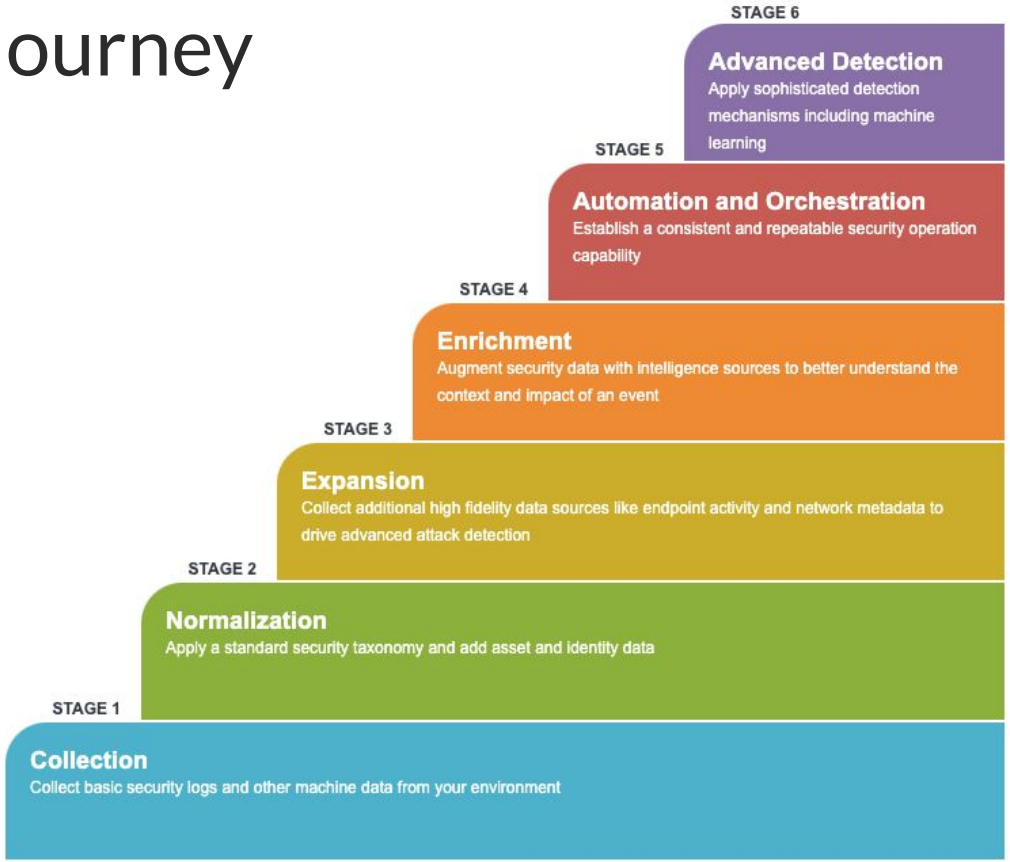
Splunk Security Data Journey

Optimise Optimise Optimise:-

Automate and **Orchestrate** where possible and appropriate

Augment your security alerting:-

Use **Advance Detections** to provide additional insight to your analysts



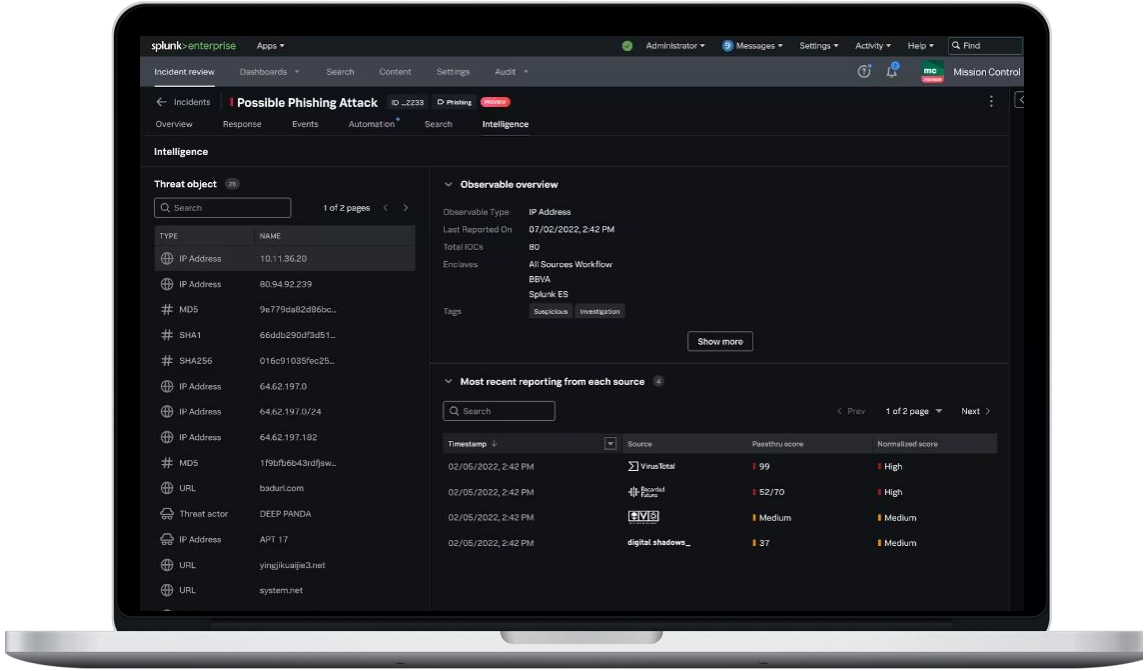
Splunk Mission Control & TIM

Unify SecOps with a single work surface

Fully rebuilt from the ground up earlier this year

Includes Access to Splunk Threat Intelligence Management

Available Now for ES Cloud Customers and Support for ES On-prem coming soon



SOAR for Security Operations

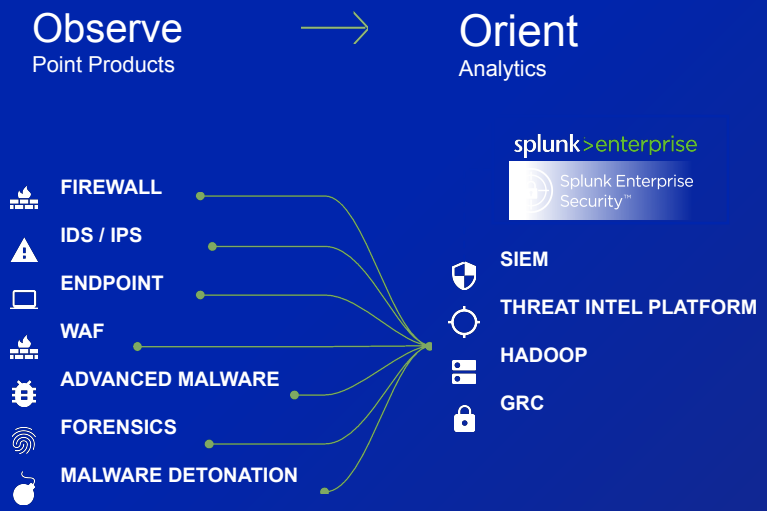
SOAR for Security Operations

Observe

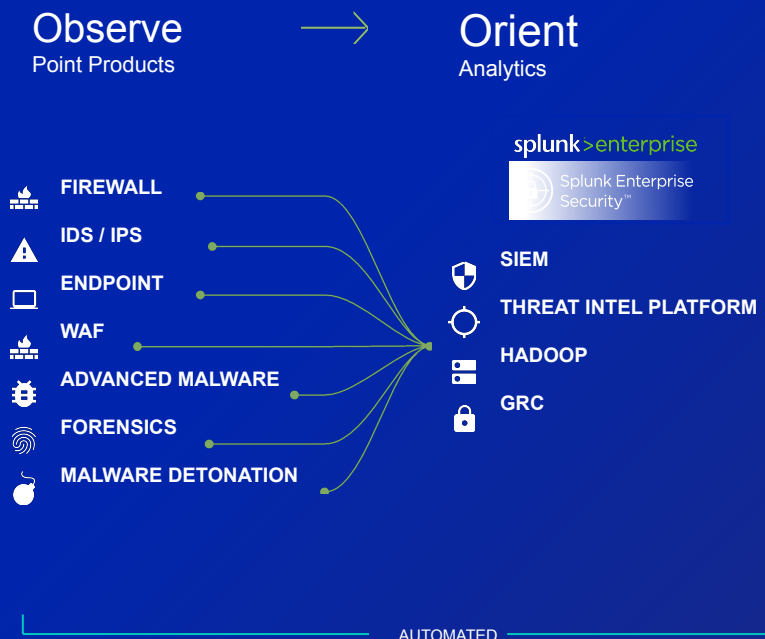
Point Products

- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

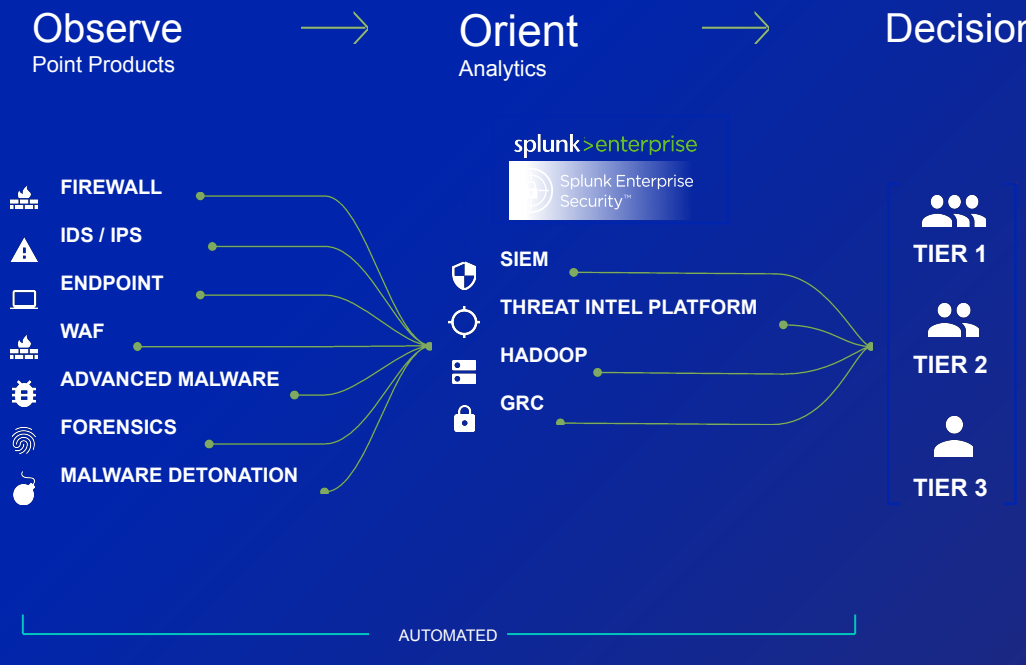
SOAR for Security Operations



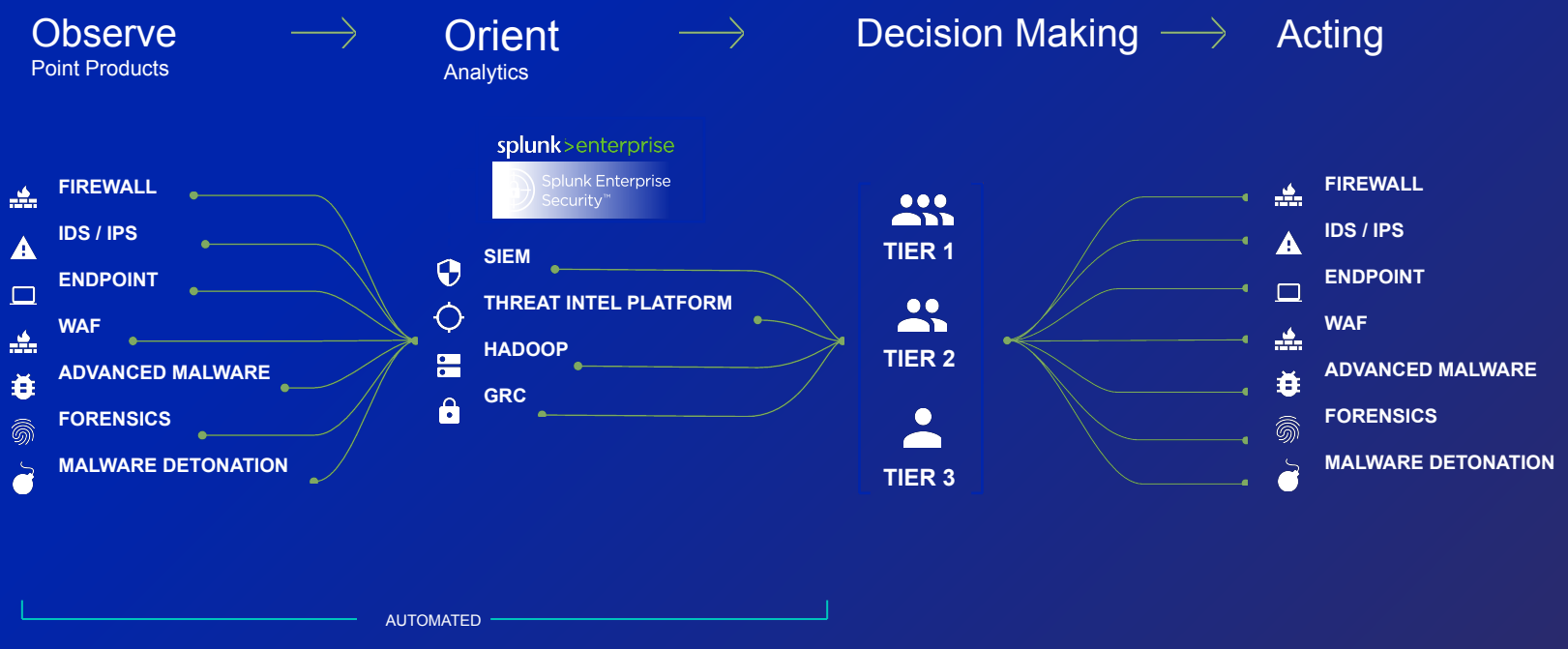
SOAR for Security Operations



SOAR for Security Operations

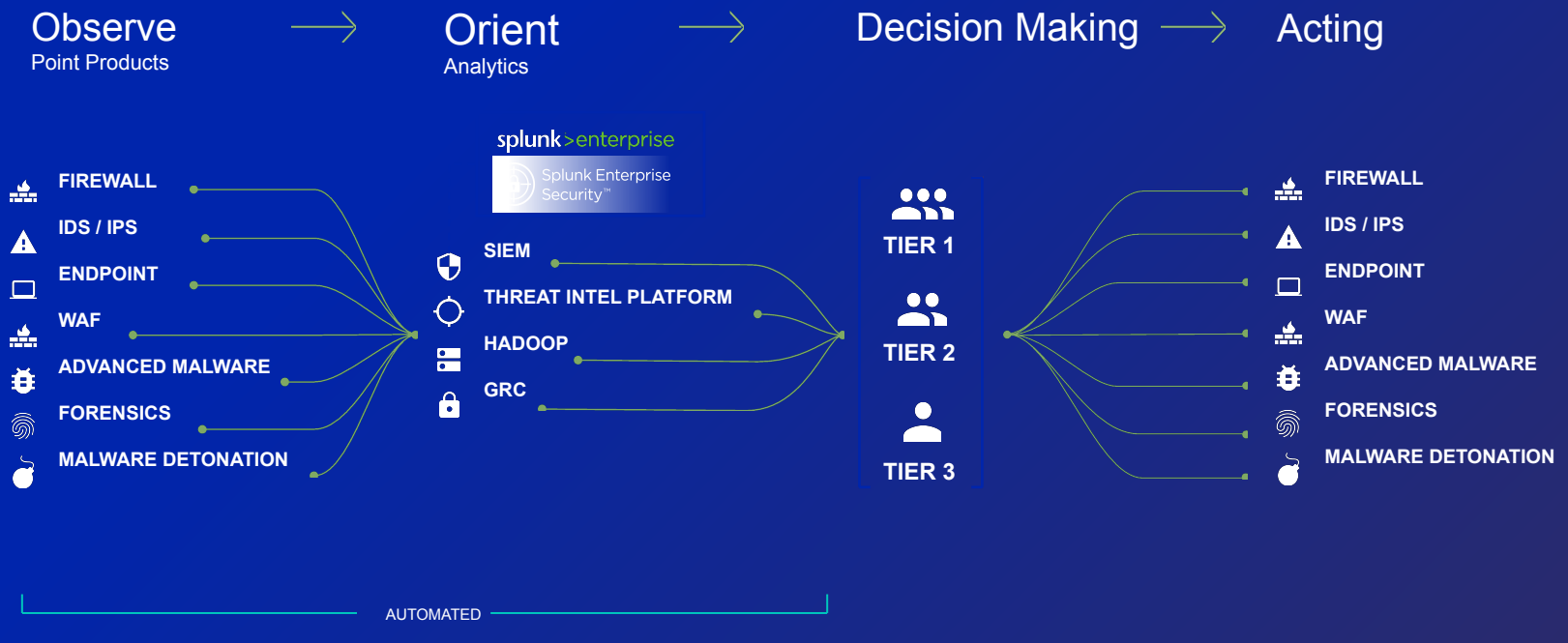


SOAR for Security Operations



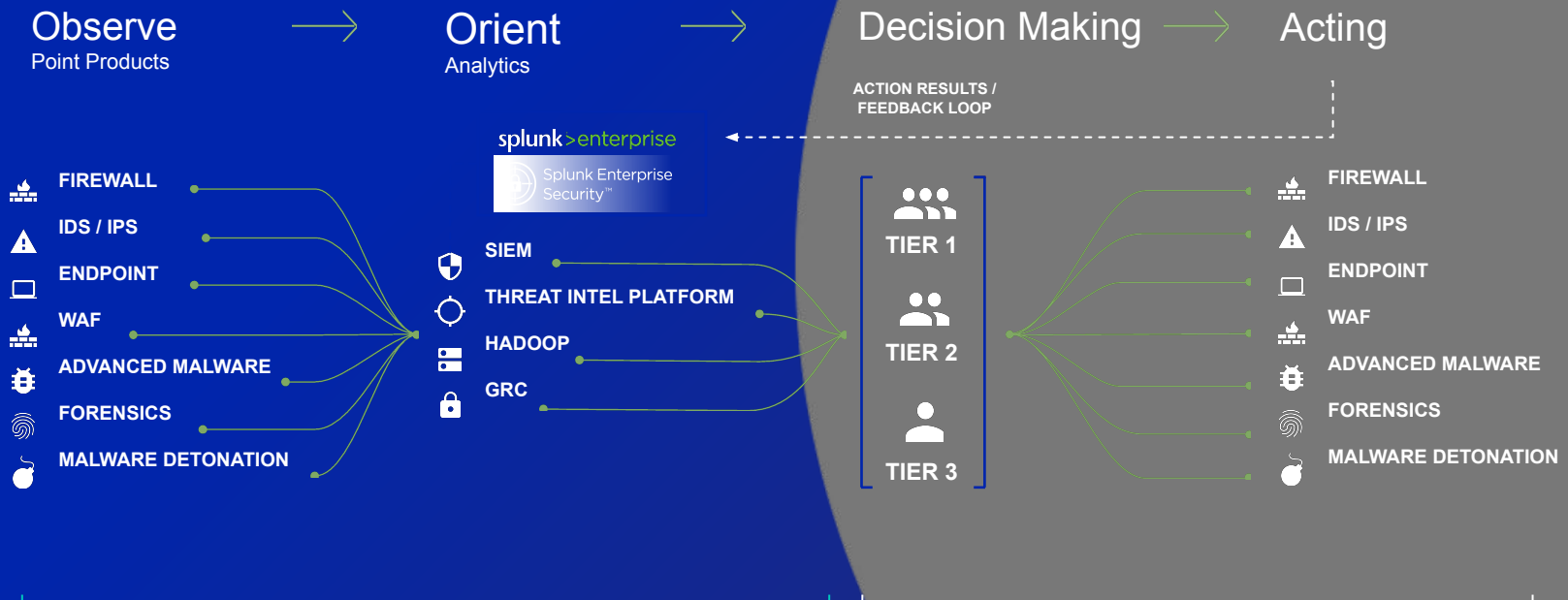
SOAR for Security Operations

Faster execution through the loop yields better security



SOAR for Security Operations

Faster execution through the loop yields better security

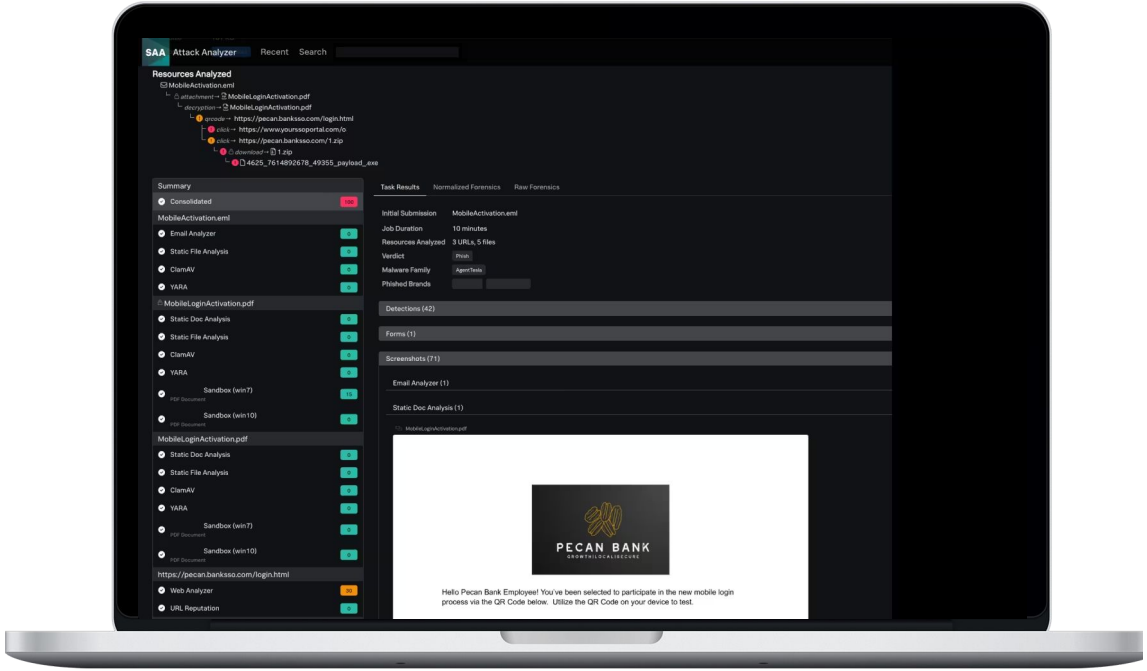


Splunk Attack Analyser

Formerly TwinWave - Next Generation Threat Analysis Platform

Detonate potential threats and automate analysis of the delivery vectors, e.g.

- Automatically scan QR codes
- Click links in email chains
- Download files
- Or even entering passwords to get at the final payload



Security Maturity

Step 1	Repeatable
Step 2	Measureable
Step 3	Manageable
Step 4	Optimising

www.somerfordassociates.com/