



Professional Services

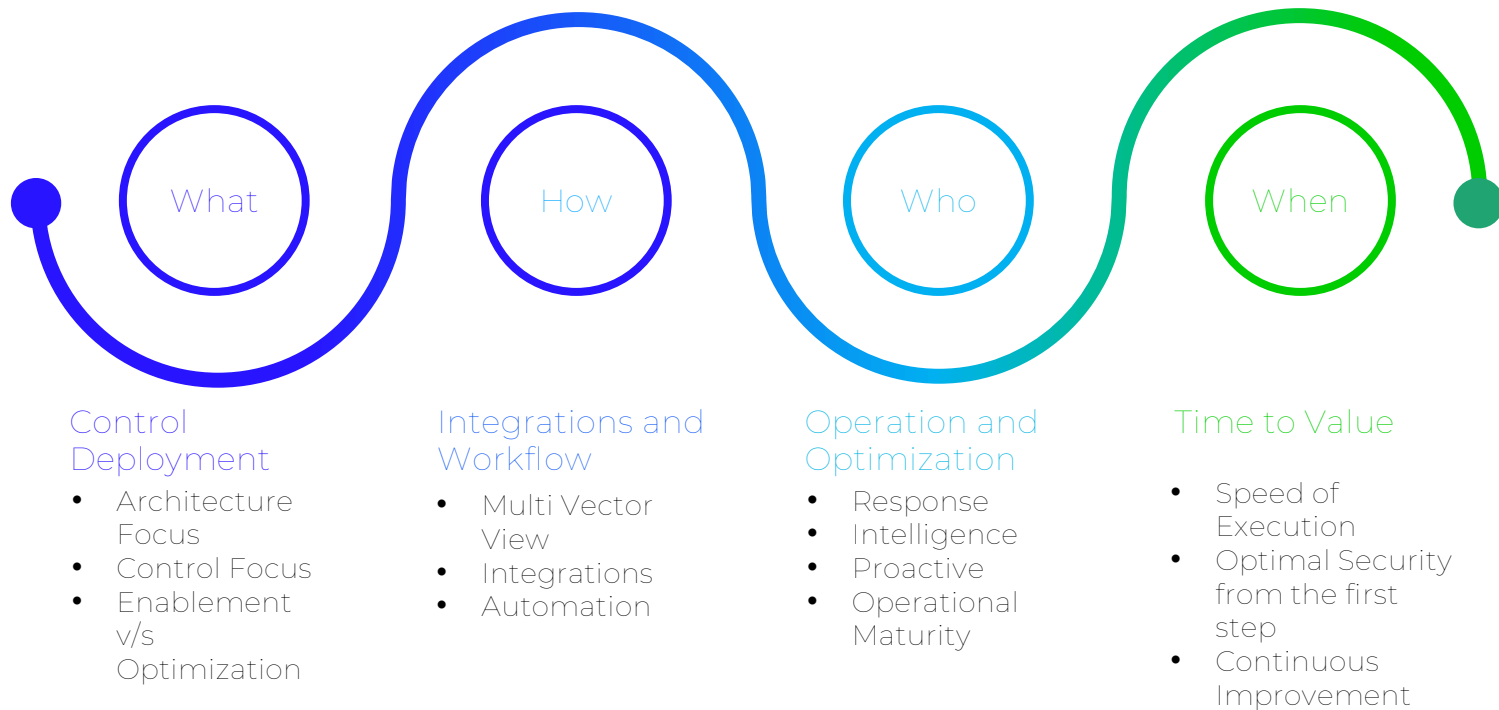
Optimizing your Security Solutions

Siju Ramachandradasan
Senior Director, EMEA
July 2, 2024



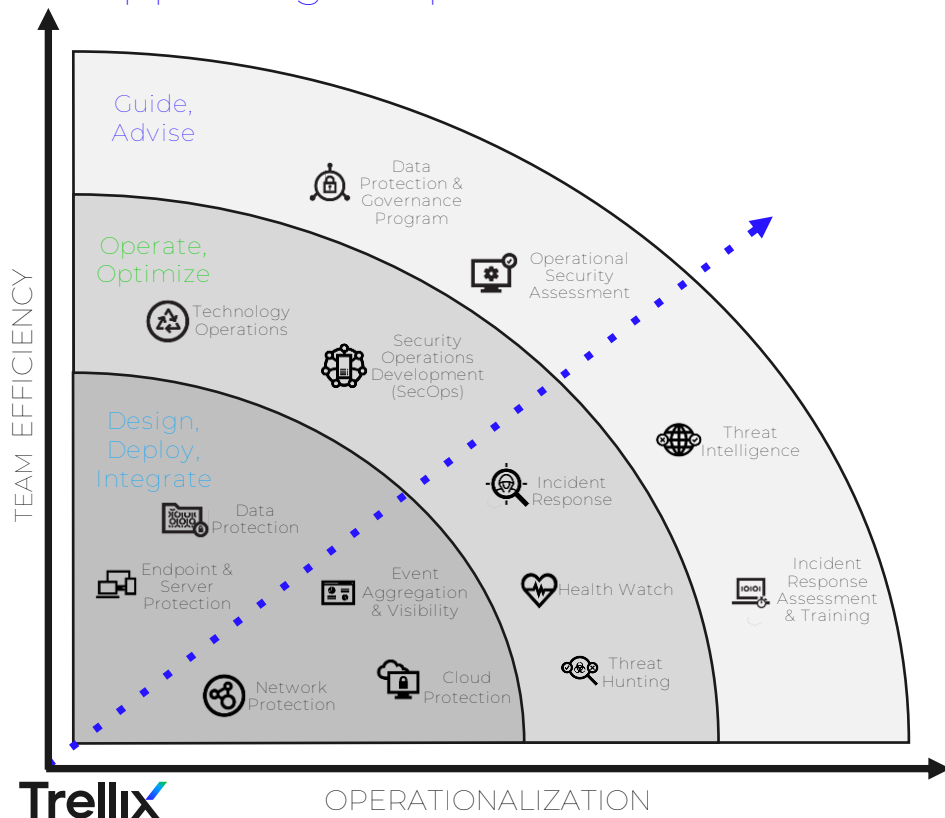
Services Landscape Evolution

Changing landscape of customer requirements



Trellix Professional Services

Supporting our partners & customer with the right level of expertise



A global organization delivering over 620,000+ hours each year helping customers protect their environments from threats

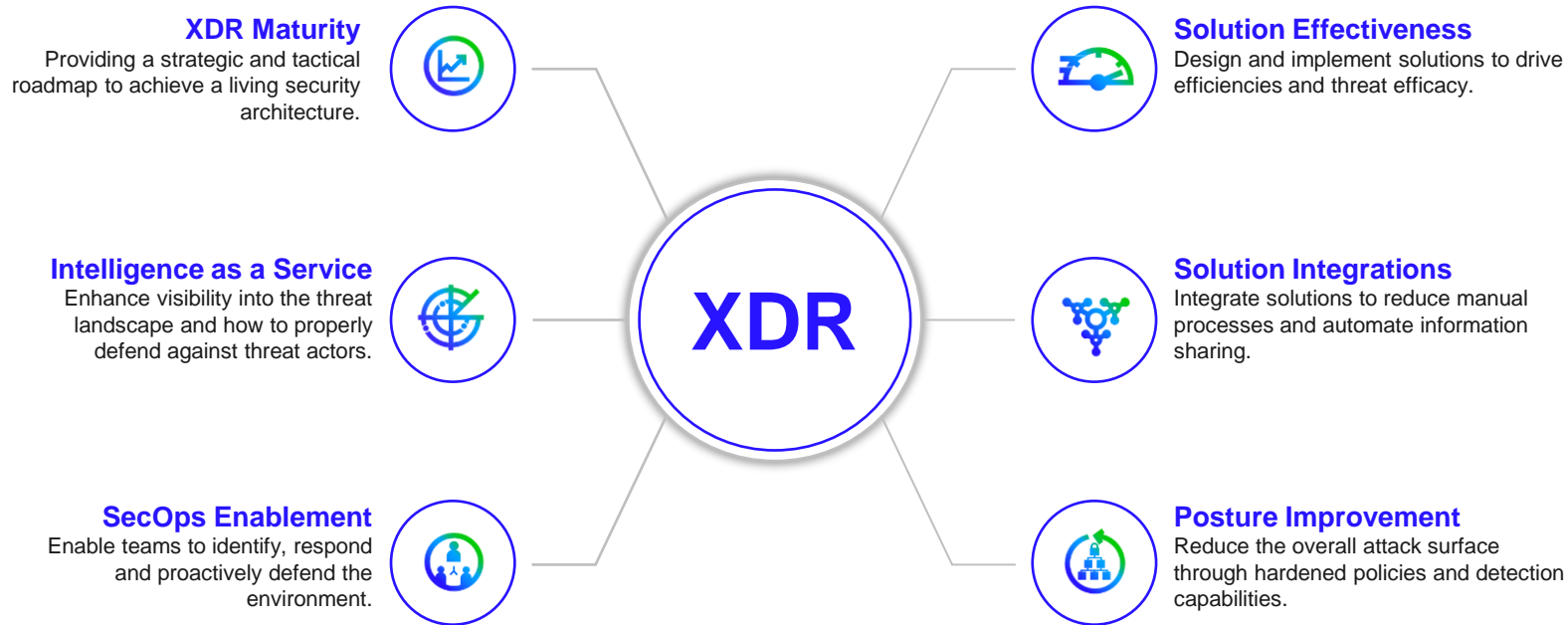
Organization characterized by:

- Culture of “Threat Protection” versus single technology subject matter expertise
- Organization that thinks like engineers and risk managers
- Organization that continues to learn and evolve in alignment with a well understood “big picture” of cyber defense

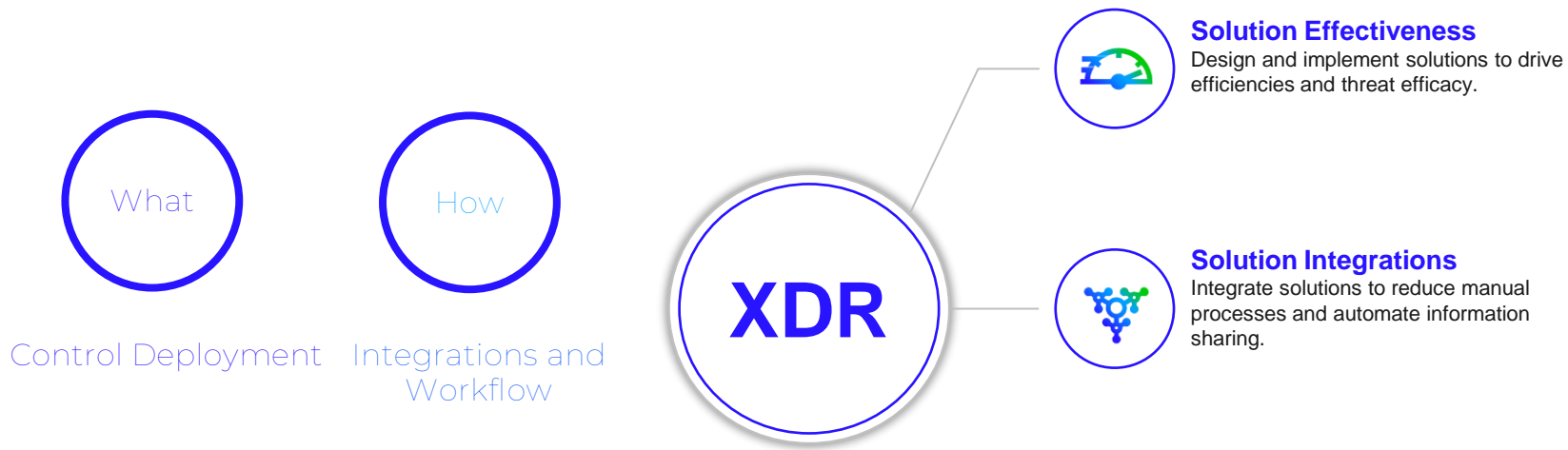
Consist of:

- Consulting Services
- Cyber Operations (TCO)
- Threat Intelligence Group (TIG)

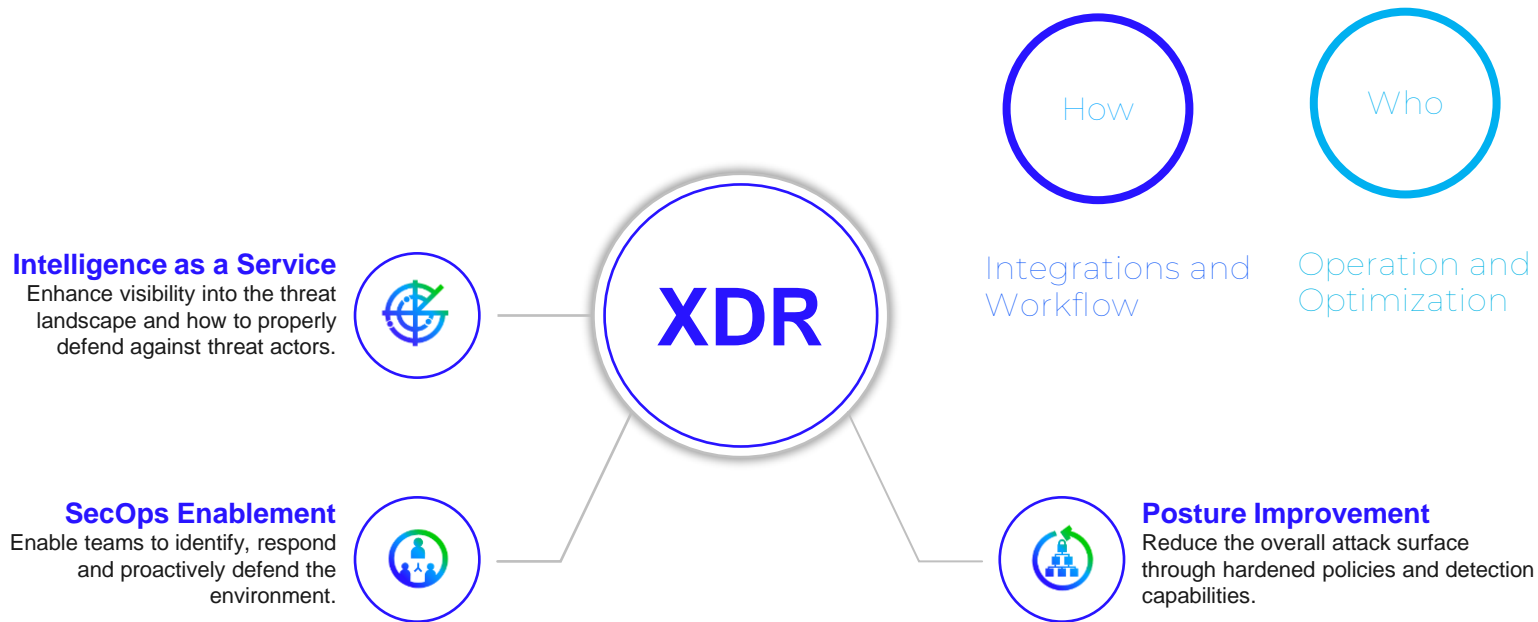
XDR Journey With Professional Services



XDR Journey With Professional Services



XDR Journey With Professional Services



XDR Journey With Professional Services

XDR Maturity
Providing a strategic and tactical
roadmap to achieve a living security
architecture.



XDR

When

Time to Value

XDR Assessment Framework



Visibility

- Network
 - On-premise
 - Cloud
 - East-West
- Endpoint
 - Physical
 - Virtual
 - Cloud
- Email
- Data
 - At rest
 - In motion
- User Behavior



Threat Intel

- Intel Sources
 - External
 - Internal
- Operational Intelligence
 - Processes
 - Capabilities
- Integration & Use
 - Security solutions
 - Intel sharing
- Automation



Detection

- Processes
 - Detection efficiency
- Technology
 - Attack vector coverage
 - Data sources
- Analytics
 - MITRE ATT&CK coverage
- Automation
- Proactive detection



Response

- Processes
 - Categorization
 - Severity
 - Playbooks
- Case Management
- Technology
 - Response vectors
 - Integration
- Automated Response Actions



Metrics

- Plan
 - Metrics identification
 - Data collection capabilities
 - Reporting capabilities
- Metrics in use
 - Current metrics
 - Reporting schedule
 - Tuning



Staffing

- Visibility
 - Tech O&M and health
- Intel Analysts
- Detection
 - 24x7 coverage
 - Capacity
 - Capabilities
 - Tech Support
- Response
 - Mobilization
 - Capacity
 - Capabilities
 - Tech Support

Trellix XDR Assessment Packaging

	Basic	Advanced	Advanced Plus	Subscription
Assessment Area				
Visibility	✓	✓	✓	✓
Threat Intelligence	✓	✓	✓	✓
Detection	✓	✓	✓	✓
Response		✓	✓	✓
Metrics			✓	✓
Staffing			✓	✓
Deliverables				
Type	Tactical	Strategic	Tactical & Strategic	Tactical & Strategic
Architecture	Current State	Current State	Current & Future State	Current & Future State
Level of Effort (Weeks)	2	3	6	

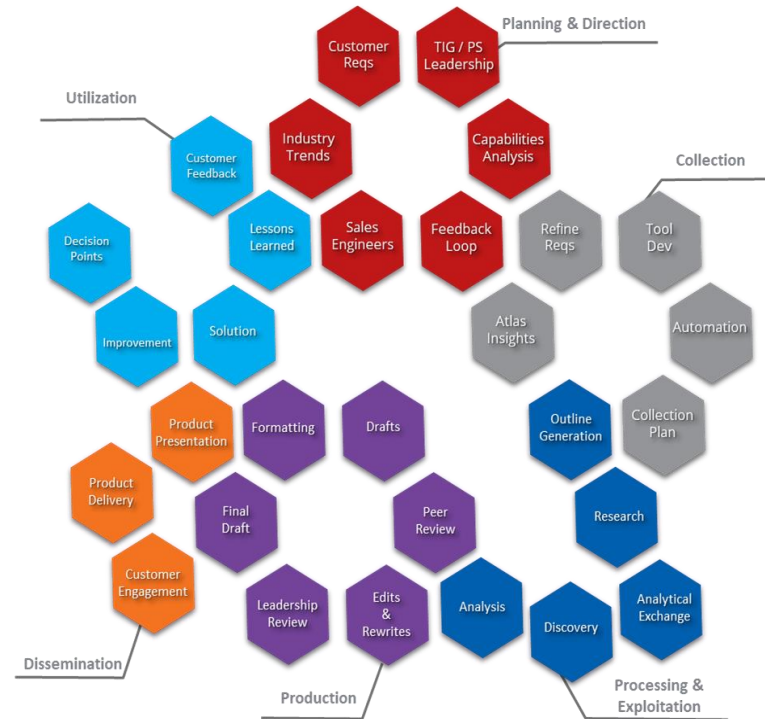
Threat Intelligence Services

Intelligence-as-a-Service

- Team of analyst
- Delivered remotely
- RFI-based research, analysis, and malware reversing

Systems

- Advanced Threat Landscape Analysis System (ATLAS)
- Threat Landscape Analysis (TLA)
- Private Global Threat Intelligence (pGTI)



Incident Response - Retainers

- Proactive and reactive incident response service delivered by Trellix PS IR security experts
- Recommended use of hours - IR Readiness Assessment and EIR hours
- Hours expire in 12 months and can be used for other Professional Services engagement

IR READINESS ASSESSMENT		EMERGENCY IR HOURS	
40-hour Incident Response (IR) Readiness Assessment is a proactive step to help you prepare for a cyberattack in your environment.		Emergency Incident Response Hours is a reactive service which provides direct access to security experts that help you effectively respond, investigate, remedy, and recover from a cyberattack.	
IR Readiness Assessment	Key Deliverables	Emergency IR Hours *	Key Deliverables
<ul style="list-style-type: none">▪ Presentation and discussion of program and expected outcome▪ Interviews with role players and stakeholders▪ Review of current IR plan▪ Understanding of product integration into the IR plan▪ Report outlining findings and recommendations▪ New and/or revised IR plan	<ul style="list-style-type: none">▪ The Trellix IR team works with your team to build a revised or new IR plan▪ End of assessment report outlines findings and recommendations for implementation of changes on IR process, including revised IR playbook▪ IR handbook review	<ul style="list-style-type: none">▪ Immediate triage of reported cyberattack (24/7/365 global-support hotline)▪ Direct access to security experts with 2-hour response Service Level Goal▪ Trellix products used to contain and mitigate▪ Immediate dispatch of security experts, if needed▪ Remediation assistance▪ Root cause analysis▪ Daily status reports and daily written investigative vulnerability finds.	<ul style="list-style-type: none">▪ Daily status report on investigative and security breach and recommended investigation strategy▪ Daily written investigative vulnerability finds and mitigation steps for implementation▪ Written final report containing all details of the Emergency IR engagement, including remediation steps and debrief on lessons learned

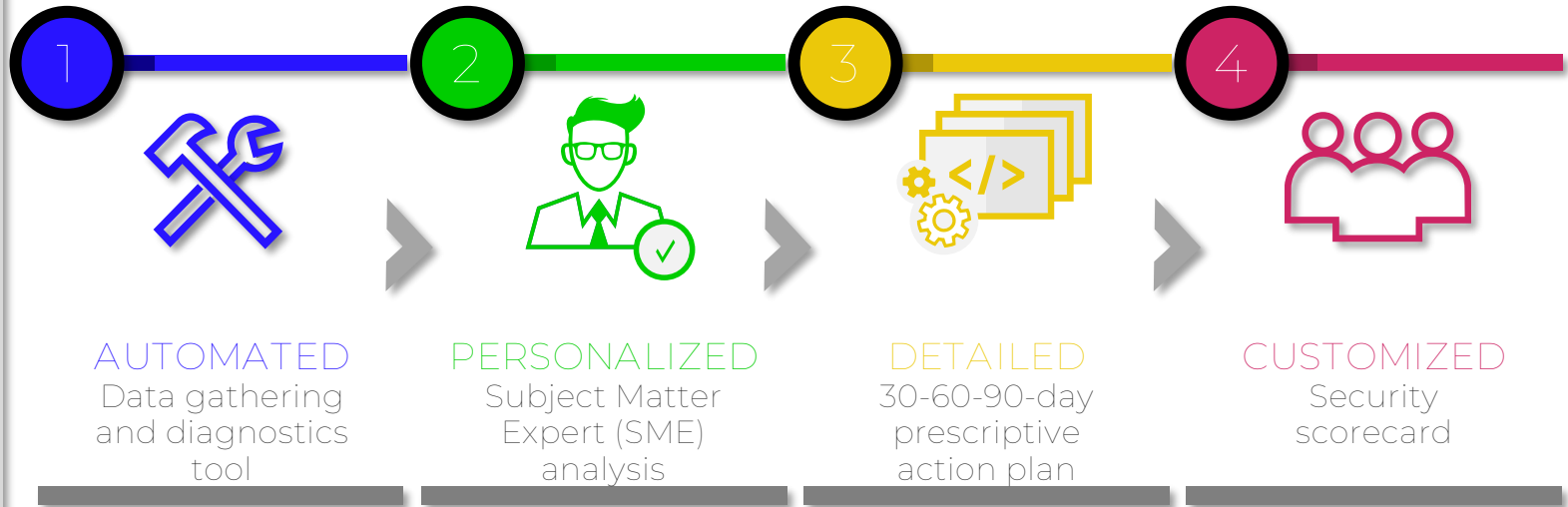
Innovation

Professional Services

////////////////////



Health Checks Made Simple



Time commitment for an engagement 2 hours

~30 min for the data collection

~1-2 hour readout session

Run a
lightweight
app

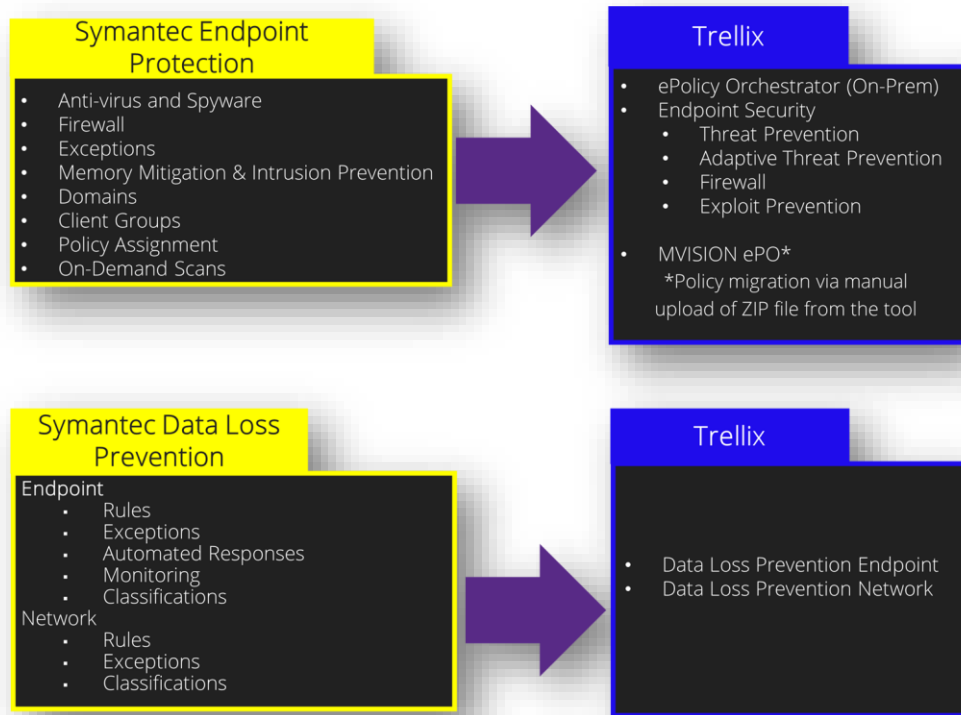
Check and
diagnose
product health

Access a portal
to view results

Review a plan
to fix issues

Receive
consultative
guidance

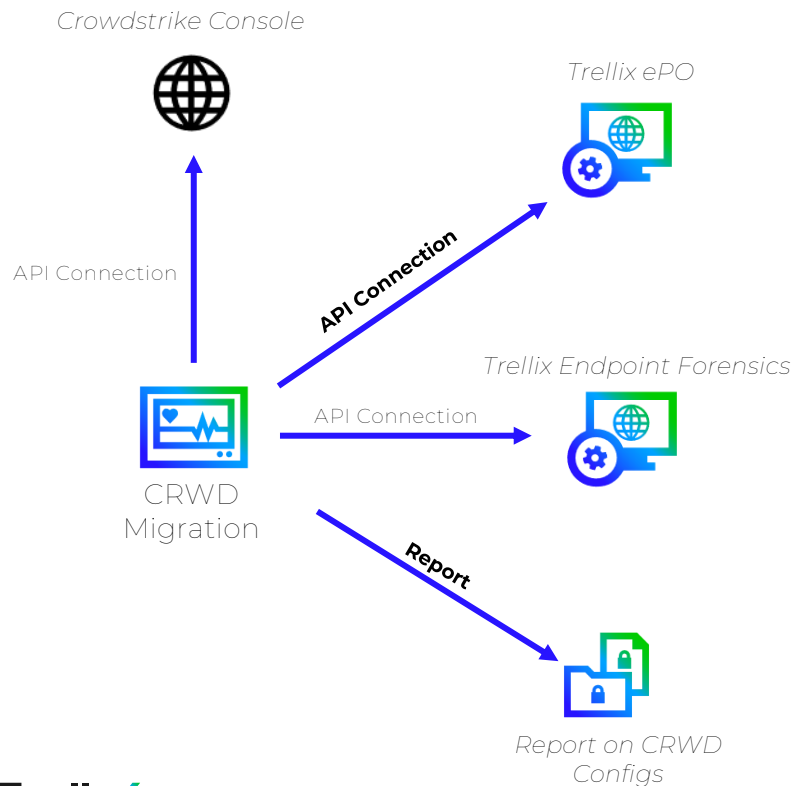
Technology Driven Migrations



Outcomes

- Migrate existing Symantec Endpoint or DLP policies/configurations to Trellix
- Provides peace of mind with existing policies
- Allows for Trellix to tune policies based on best practices

Technology Driven Migrations



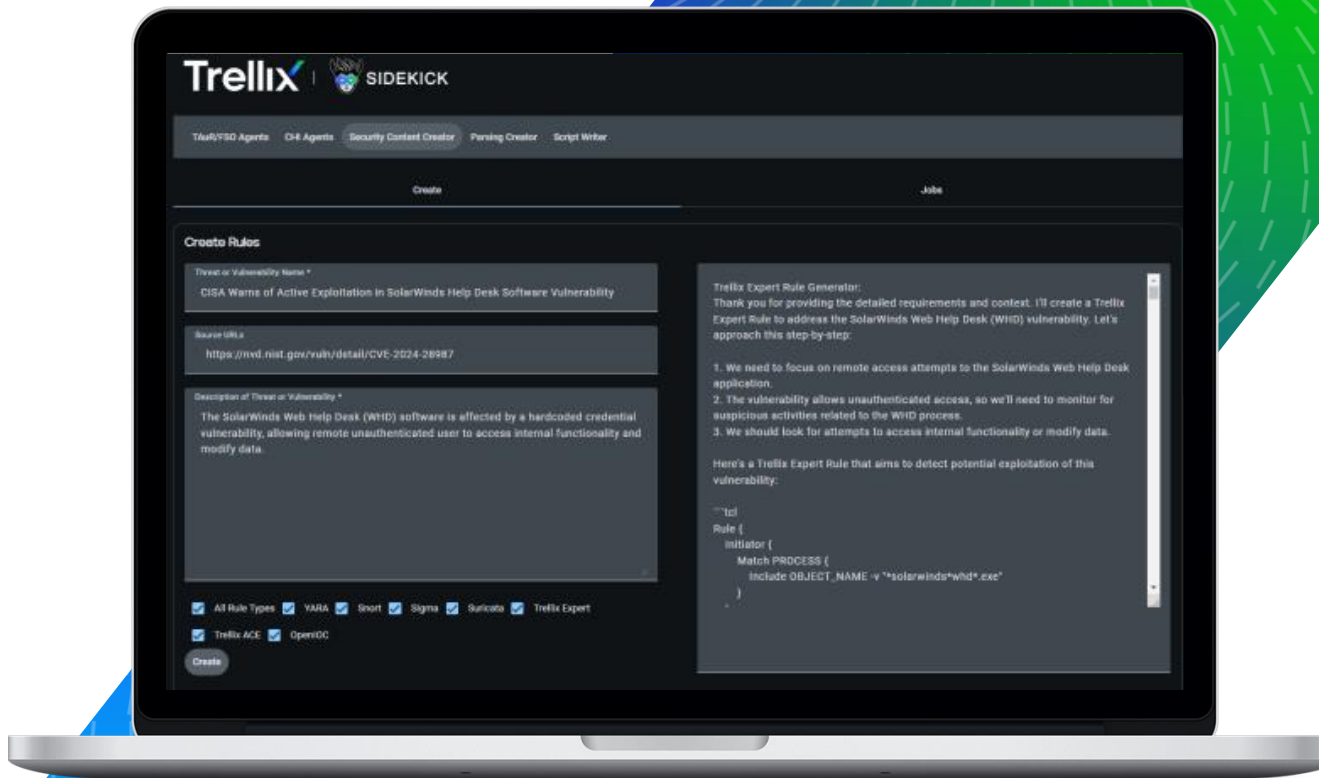
1. Application connects to the Crowdstrike Console
 - Uses customer provided Client ID and Client Secret token
2. Exports configurations, hosts and hosts sets
3. User enters their Trellix environment details
 - ePO:
 - IP Address, Username and Password
 - HX Appliance:
 - IP Address, Username and Password
4. Converts the CRWD configurations into Trellix format
5. Imports the converted configurations into the Policy catalog
 - Converted policies will have the leading name:
 - CRWD Conversion
6. Imports devices objects into ePO System Tree and groups
7. Created a report locally on the configurations exported from Crowdstrike and Trellix features they were converted too

SideKick

Internal GenAI based tool



Scripts
Security Content
Parsers
Yara Rules
Expert Rules



How we can help !

1

Tag Team

Let's work together to ensure our customers get the quickest route to value. We keep innovating with your support.

2

Reduce Risk

Let's complement our expertise and yours to ensure we reduce the engagement risks..

3

Involved throughout the journey

It is not a one stop deploy. Let's drive value and continuously mature the customer deployment through innovative solutions and services.



Trellix