RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART2-W02**

Being Open to a Zero Trust Future

Chris Meenan

VP, IBM Security Product Management

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single products, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services re immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

Market needs innovation and simpler, consumable, and more effective security.

01

Organizations are undergoing rapid digital transformation

Shift to hybrid cloud

Infrastructure distributed across hybrid cloud, edge, IoT and OT

Regulatory and privacy demands

As data is shared, regulations and end-users demand more control

Remote workforce

Employees accessing data from anywhere, using any device

Evolving threats

Increasing ransomware and other sophisticated attacks

Security is fragmented

- 66% of security teams do NOT share their data
- 45% of security teams require security engineers to hand wire integrations
- 1:1 ratio of security analysts and integrators hired equally, no improvement since 2019

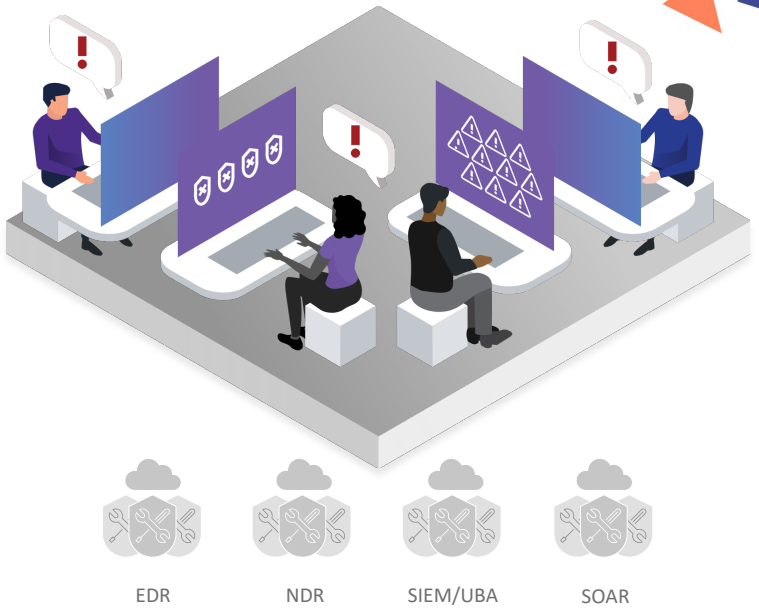
Complexity creates adversary opportunity

Poor visibility

Disconnected tools

Outdated detection

Struggle to keep up



59% of organizations say cybersecurity has become more difficult over the last two years

“Open Security”

[noun] The sharing of security data analytics (feeds, intel, etc.), security methods or best practices, adhering to and or promoting standards and contributing or consuming code developed to secure or protect users, data, endpoints, workloads and more.

02

CLOSED Security is a roadblock

Proprietary technology

Vendor-specific rules and content

Fragmented tools and interfaces

Slow and resource constrained

OPEN Security is an accelerator

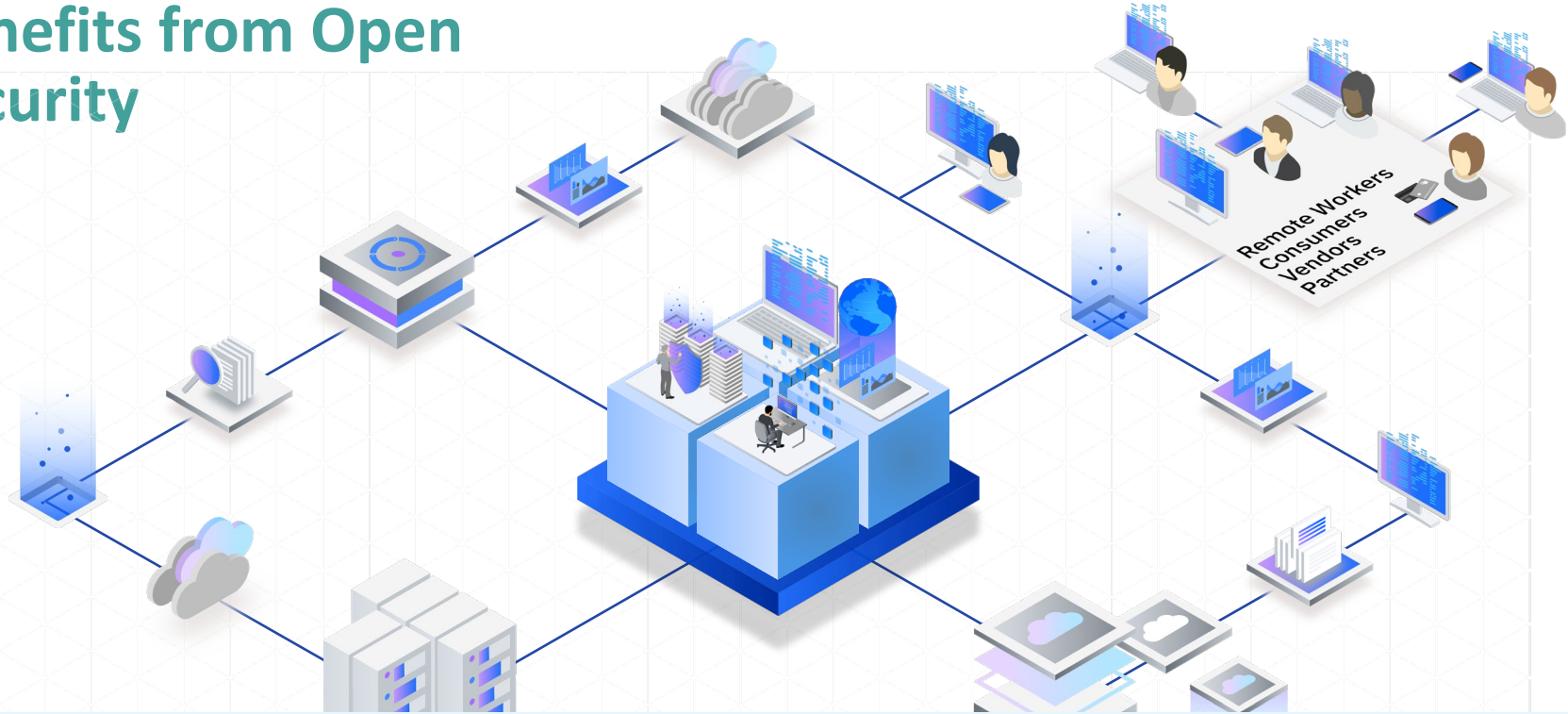
Open standards and interoperability

Community-led innovation, expertise

Shared data and user experience

Accelerated stream of innovation

Benefits from Open Security



Trust and transparency

- Exchange with domain exports
- Contribute to research and development
- Obtain feedback and comments

Speed and awareness

- Early access to novel technologies
- Learn about tech and threat trends
- Reduce blind spots and breaches

OCA was founded to promote and support open security

IBM Security · McAfee · CIS Center for Internet Security · cybereason · CYBERNB CIPnet · CYDARM · CYWARE
EclecticIQ · f5 · [redacted] · RAPID7 · SafeBreach · SAIC
VMware Carbon Black

Who

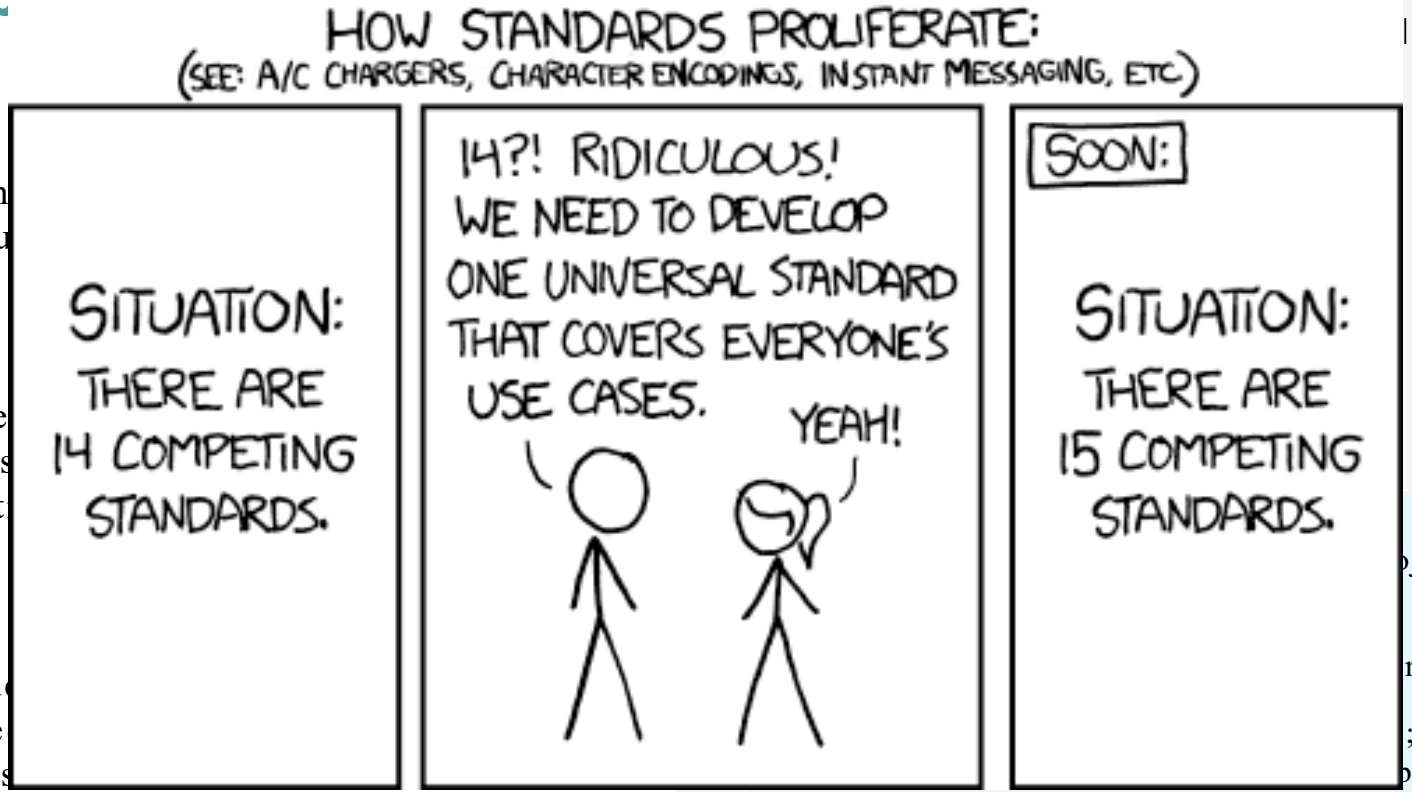
Global like-min
end users, thou

What

Support an ope
where products
insights, analyt

How

Open-source d
mutually agree
and procedures



Key OCA initiatives

STIX Shifter

- Cybersecurity toolchain for unified query and response using the STIX 2.x standards
- Goal: Standardize on one query language and response data model for all data sources
- 29 data sources supported (to date)
- Sponsored by IBM

Kestrel Threat Hunting Language

- Builds on STIX Shifter to create a unified threat hunting language and tool that works across all supported data sources
- Out-of-the-box machine learning and analytics, integrations with Jupyter Notebooks for GUI
- Sponsored by IBM

PACE – Posture Attribute Collection and Enumeration

- Bring posture collection standards up to date with the cloud era
- Instantiation of the IETF SACM working group's architecture with SCAPv2
- Sponsored by CIS, NSA, and McAfee

WORKGROUPS

Indicators of Behavior Sharing

- Focused on the challenge of moving detections to Indicators of Behavior (IoB)
- How to collaborate on and share IoB-based detections between products and tools
- Chaired by Cybereason, JHU-APL, IBM

OCA Ontology

- Creating a unified ontology for cybersecurity information to standardize encoding on data fabrics, APIs, etc.
- Original "Open DXL" ontology expanded to encompass other messaging fabrics
- Chaired by SAIC, NIST, McAfee

Zero Trust Architecture

- Creating and refining OCA technologies to enable Zero Trust architectures
- Creating a unified reference architecture for all aspects of enterprise cybersecurity operations
- Chaired by IBM, NIST, VMWare, others

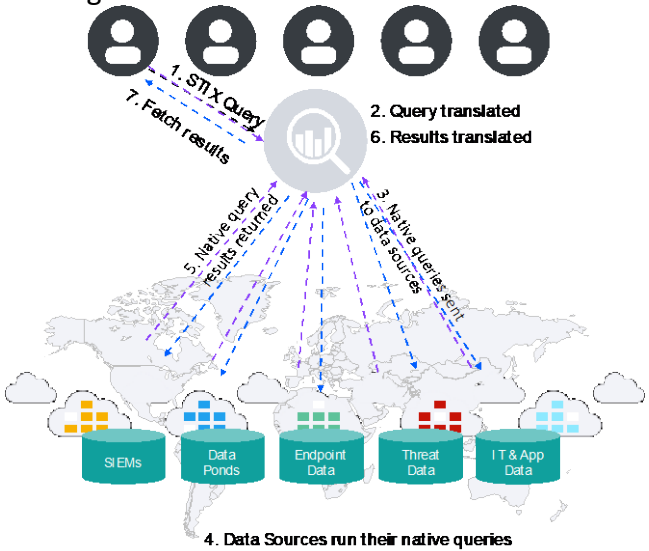
Detecting threats across security analytics tools

- Problem
  - Security data is stored across a wide variety of silos
  - No widely-adopted standard for running queries and enrichments across tools and schemas

- Solution
  - We need to normalize for detects, hunts and response
  - Submit one pattern to query all security products at once
  - See the query results in one normalized format
  - Extensibility, portability / re-use (skills), collaboration

STIX-shifter: Federated Data Access

- Enable analysts to exchange information in a Structured Threat Information eXpression (STIX) across multiple security domains
- STIX 2 Patterning for stateful detections use cases, matching use cases and custom use cases.

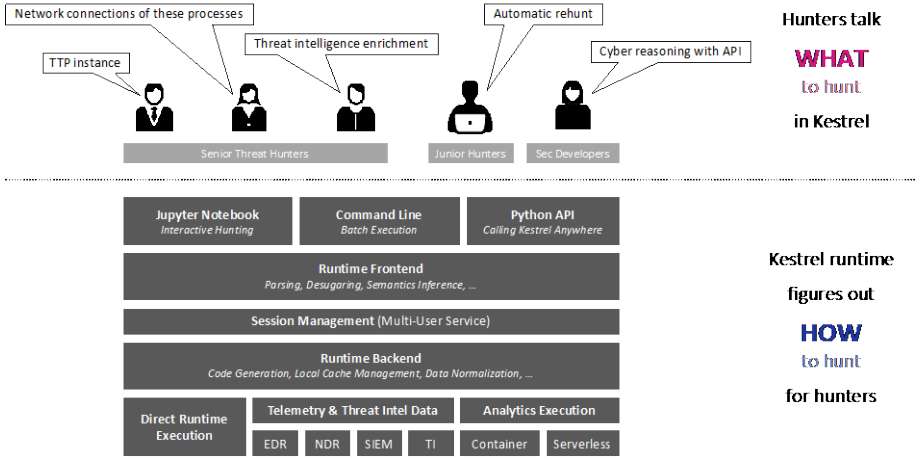


Evolve to proactive security with threat hunting

- Problem
  - Hunting approaches are primarily human-driven and require deep technical, systems, and organizational skills
  - Lack of systematic methodology and access to fragmented security data makes threat hunting difficult
- Solution
  - Develop a systematic game plan that works across multiple products in a heterogeneous environment
  - Create a collaboration method for threat hunters to leverage the power of multiple minds coming together

Kestrel – An open threat hunting approach

- Kestrel enables threat hunters to compose hunts in an open expression and abstracts heterogenous environment interfaces
- Built on Stix-Shifter – an open approach for federated search
- Leverages ML to execute tedious tasks, allowing threat hunters to focus on more pressing tasks



A simple threat hunting example

Carbon Black

```
( ( parent_name:winword.exe OR
    parent_name:outlook.exe OR
    parent_name:excel.exe
  ) AND
  ( process_name:powershell.exe
OR
    process_name:cmd.exe OR
    process_name:wmic.exe OR
    process_name:cscript.exe
  )
)
```

Threat Hunters must:

- Understand the threat TTP
- Determine relevant EDR
- Obtain access to Carbon Black
- Learn Carbon Black's APIs
- Learn how to script these APIs
- Convert return data to usable format
- Python scripts to automate the hunt

..and then do it all again

Crowd Strike

```
event_simpleName=ProcessRollup2 (FileName=node.js OR
FileName=nginx OR FileName=apache)
    | dedup aid TargetProcessId_decimal
    | rename FileName as Parent
    | rename CommandLine as ParentCmd
    | table TargetProcessId_decimal Parent ParentCmd
    | join max=0 TargetProcessId_decimal
      [ search event_simpleName=ProcessRollup2 FileName=bash
            OR FileName=zsh
            OR FileName=csh
            OR FileName=sh
        | rename ParentProcessId_decimal as
TargetProcessId_decimal
        | rename MD5HashData as MD5
        | rename FilePath as ChildPath
        | dedup TargetProcessId_decimal MD5
        | fields TargetProcessId_decimal FileName CommandLine
]
    | table Parent ParentCmd FileName CommandLine
```

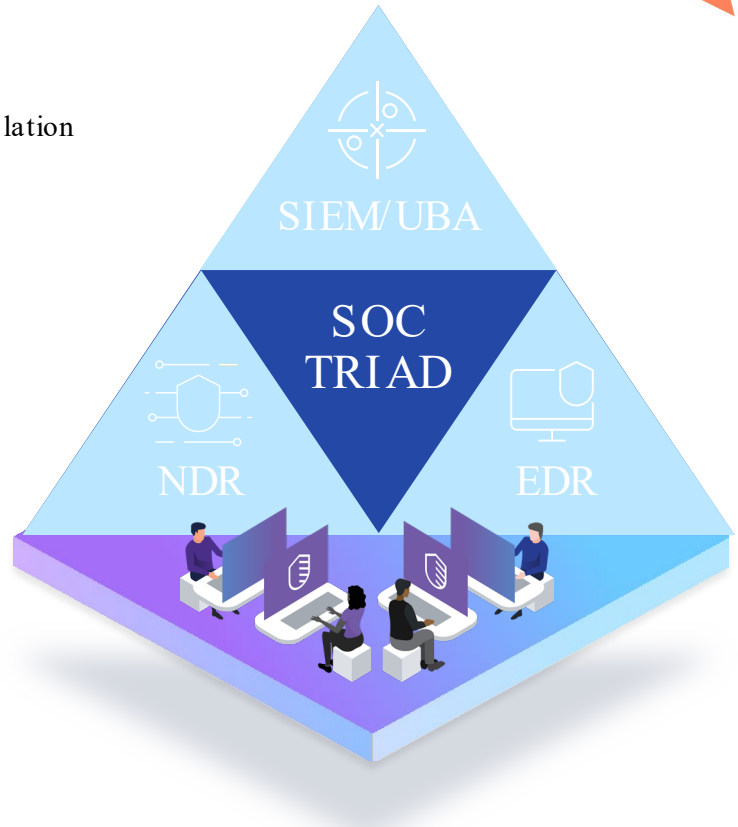
Benefits in using Kestrel…

```
GET process FROM myEDR WHERE [process:name IN ('powershell.exe', 'cmd.exe', 'wmic.exe', 'cscript.exe')
                AND process:parent.name IN ('winword.exe', 'outlook.exe', 'excel.exe')]
```

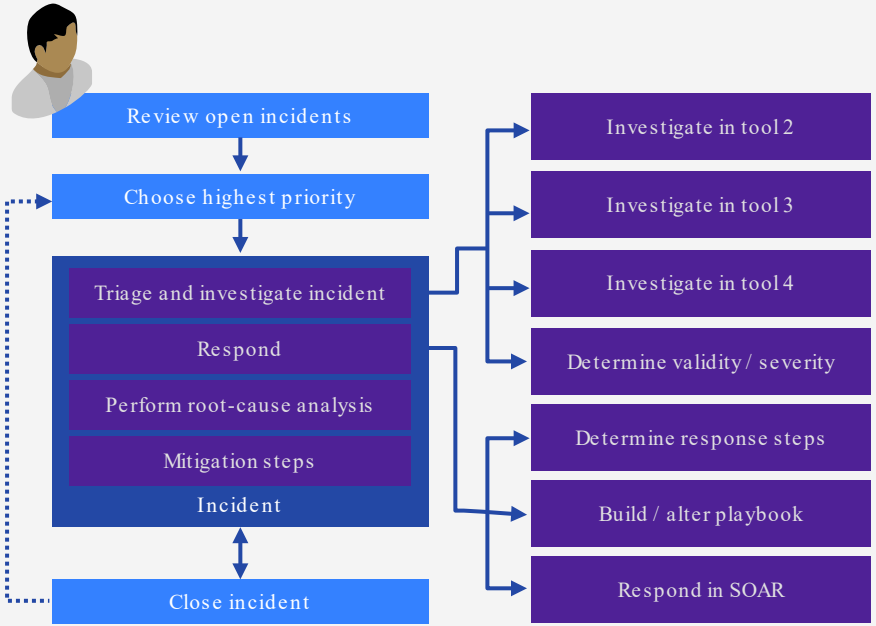
- Simple yet powerful language that's tailored for threat hunting
- Unified across all environments and tools
- Shareable framework to accelerate knowledge sharing and hunt re-use
- Extensible with external machine-learning and analytics

Modernization requires visibility and advanced analytics

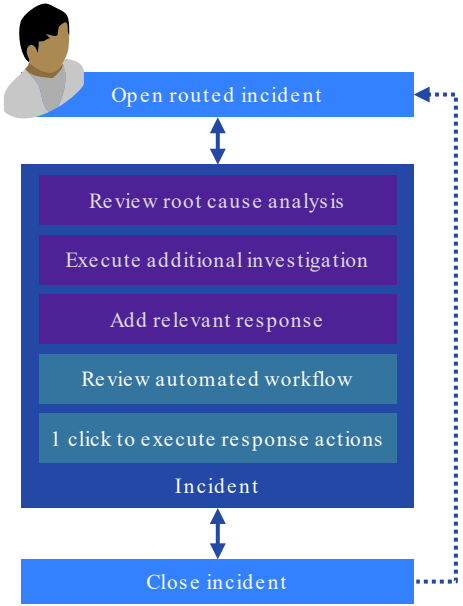
User and entity threat analytics with SIEM/UBA	Behavioral and rule-based detection and correlation of malicious activity through real-time analysis of log data across the enterprise
Endpoint Detection and Response (EDR)	Behavioral detection and prevention of malicious activity across endpoints and mitigate and respond to threats remotely
Network Detection and Response (NDR)	Behavioral detection based on malicious network activity and SIEM/UBA and EDR gaps to provide critical insights to prioritize remediation



Security analysts typical workflow complexity



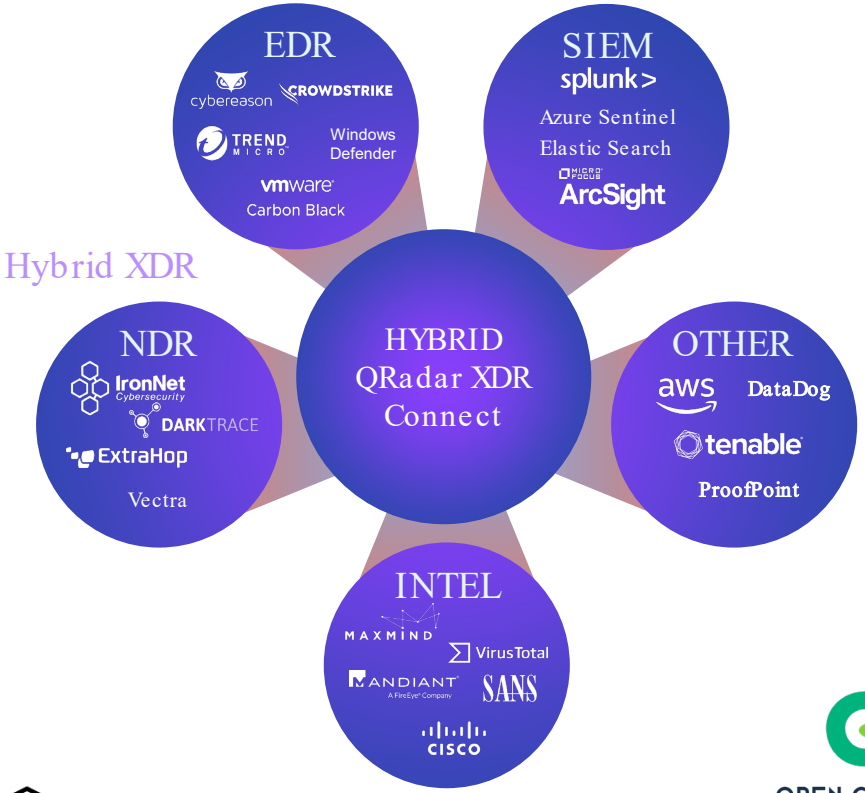
Simplified and integrated detection and response workflow

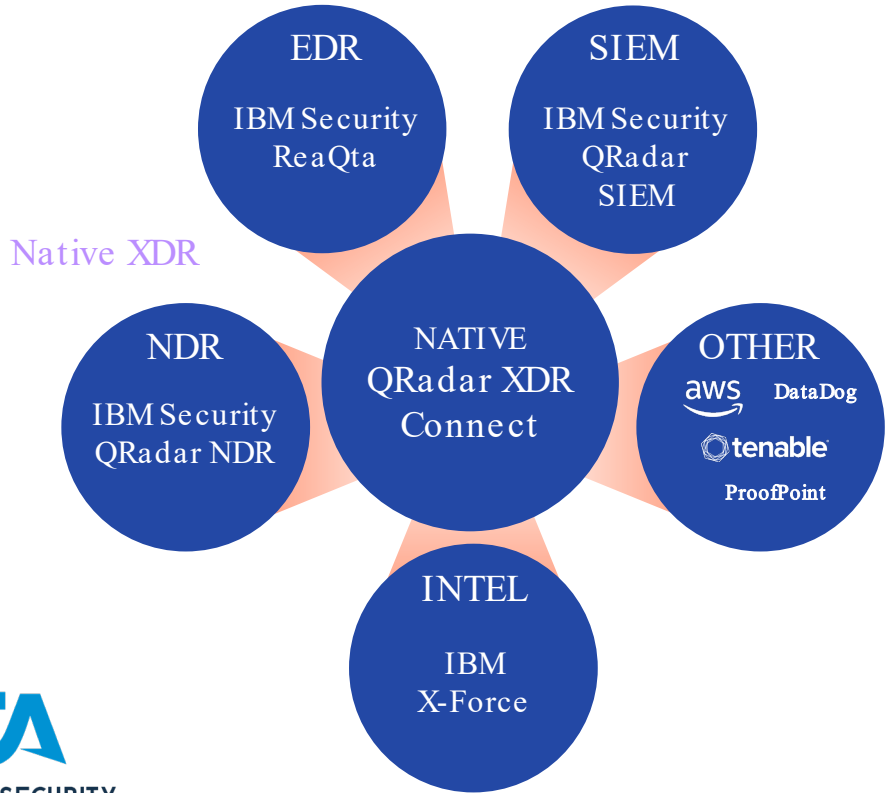


- Fewer, more accurate alerts with an open scalable approach
- Leverage existing tools and avoid vendor lock in
- Streamlined workflow, reduced manual effort thanks to automation
- Pre-built detection and response so teams can protect your organization, even without deep security expertise

IBM Security

Enabling flexible hybrid or native XDR depending on what you need

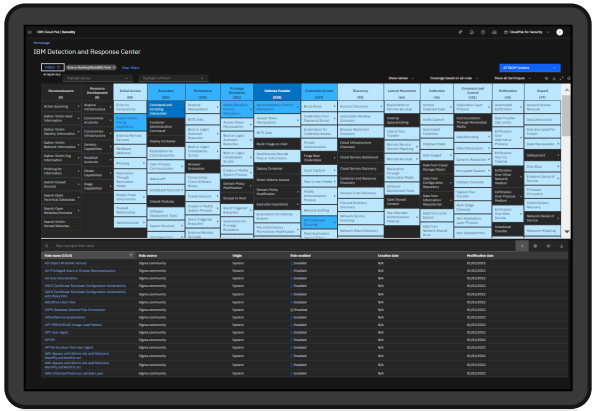




OPEN CYBERSECURITY ALLIANCE

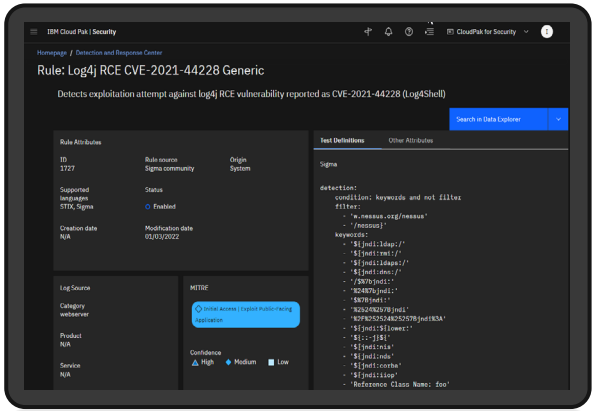
Open Security in practice - QRadar XDR Connect

MITRE ATT&CK™



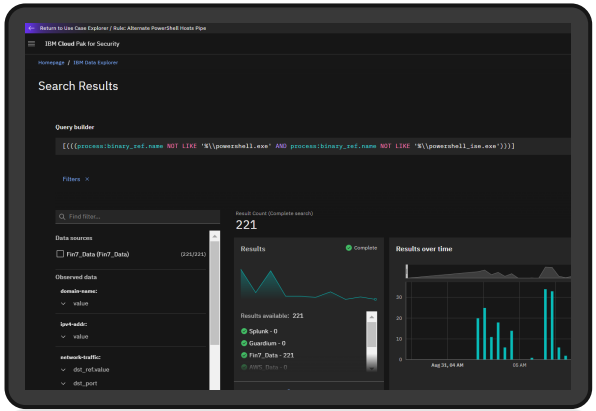
- Common attack surface controls
- Enables prioritization and measurement

SIGMA



- Common language for detection
- Huge community accelerating detection and protection

STIX SHIFTER

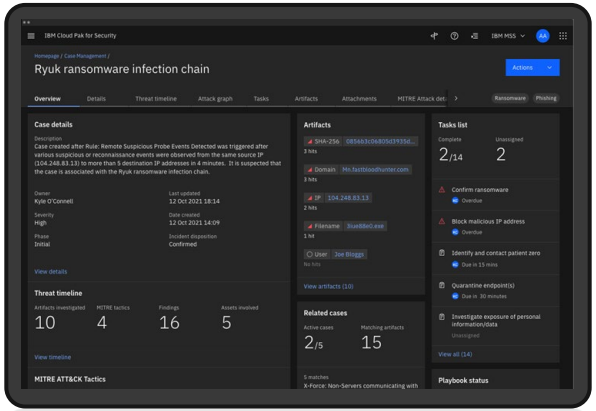


- Common investigation and hunting
- Choose what data storage tools make sense for you

Seamlessly Integrated Workflow

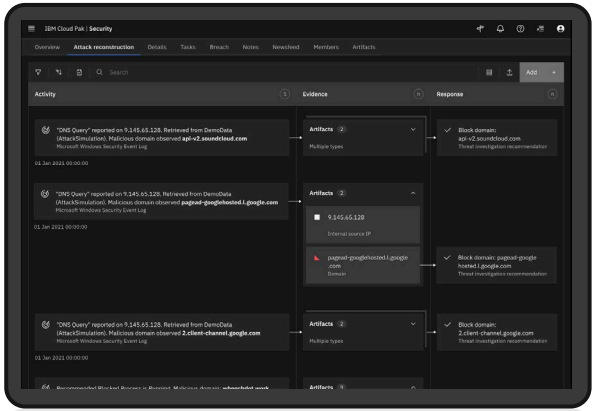
Open Security in practice - QRadar XDR Connect

OpenDXL



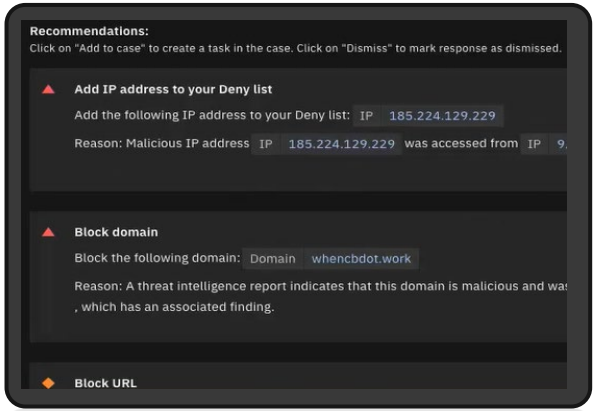
- Unified, correlated view of malicious activity
- Leverage detection capabilities from cloud, endpoint, app, data, etc.

SIGMA + STIX SHIFTER



- Automated data mining and timeline creation
- Force multiple you security team

OpenC2



- Recommended next steps and actions
- Respond more quickly and consistently

Seamlessly Integrated Workflow

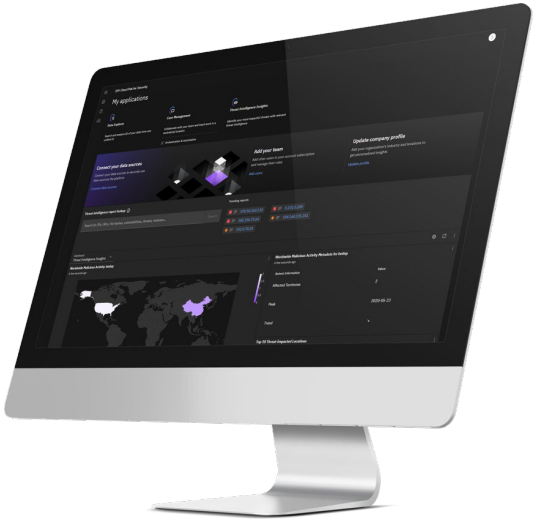
Open security enables the future

UNIFIED — Single user experience across tools and teams

INTELLIGENT — Analytics, Automation and AI built for detecting threats and analyst productivity

CONNECTED — Integration with your existing tools or IBM's

OPEN — Adaptable architecture to help avoid lock-in



QRadar XDR

On premise | Hybrid Cloud | SaaS | aws | Azure | Google Cloud | IBM Cloud

Apply What You Have Learned Today

- This week:
  - Stop by the IBM Security booth and have a one-on-one conversation with our IBM Security QRadar subject matter experts