RAPID7 VS IBM QRADAR SAAS

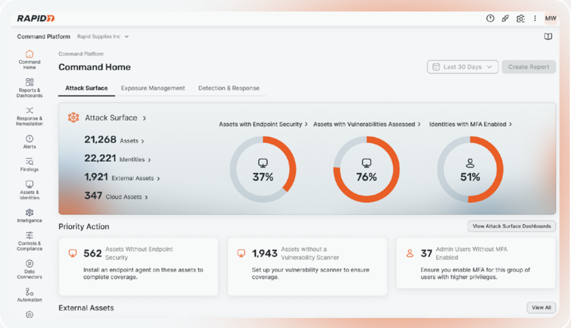
Incident Command is the Right Choice for QRadar Customers Facing Forced Migration

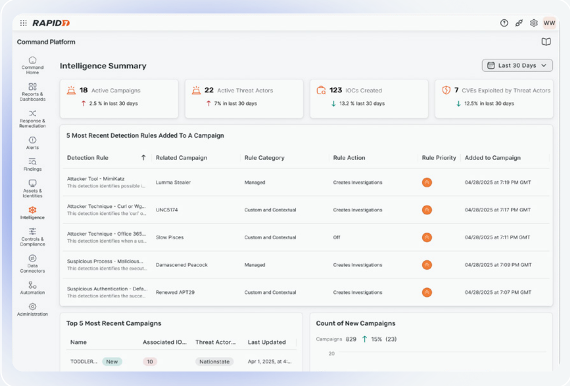
The SIEM market is undergoing a major transformation, driven by the need to combat escalating and increasingly sophisticated cyber threats while enabling real-time detection. Modern Security Operations Centers (SOCs) must now manage an unprecedented and continuously expanding volume of security and IT system logs.

For teams making the shift from the QRadar SIEM, the choice goes beyond features to trust and usability. Analysts need tools that simplify their work and strengthen security. Rapid7 delivers a full-featured Next-Gen SIEM with full visibility across the environment, mapping detection coverage to the attack surface, and scaling teams with AI trained on thousands of hours of expert MDR delivery. With Rapid7, customers gain continuity and a clear path forward built on stability, innovation, and the confidence of a proven security partner.

Unified AI-Native Security Operations Platform

Unlike QRadar's fragmented and complicated, multi-tool approach, Incident Command delivers detection, exposure visibility, threat intelligence, digital forensics and incident response (DFIR), and attack surface management (ASM) in a single platform that provides a seamless, end-to-end security detection lifecycle, enabling analysts to focus on high-value threat hunting and rapid response.





5 Most Recent Detection Rules Added To A Campaign

Detection Rule ↑	Related Campaign	Rule Category	Rule Action	Rule Priority	Added to Campaign
Attacker Tool - MimiKatz This detection identifies possible i...	Lumma Stealer	Managed	Creates Investigations	●	04/28/2025 at 7:19 PM GMT
Attacker Technique - Curl or Wg... This detection identifies the 'curl' o...	UNC5174	Custom and Contextual	Creates Investigations	●	04/28/2025 at 7:17 PM GMT
Attacker Technique - Office 365... This detection identifies when a us...	Slow Pisces	Custom and Contextual	Off	●	04/28/2025 at 7:11 PM GMT
Suspicious Process - Malicious... This detection identifies the execut...	Damascened Peacock	Managed	Creates Investigations	●	04/28/2025 at 7:09 PM GMT
Suspicious Authentication - Defa... This detection identifies the succe...	Renewed APT29	Custom and Contextual	Creates Investigations	●	04/28/2025 at 7:07 PM GMT

Top 5 Most Recent Campaigns

Name	Associated IO...	Threat Actor...	Last Updated
TODDLER... New	10	Nationstate	Apr 1, 2025, at 4:...

Count of New Campaigns

Campaigns 829 ↑ 15% (23)

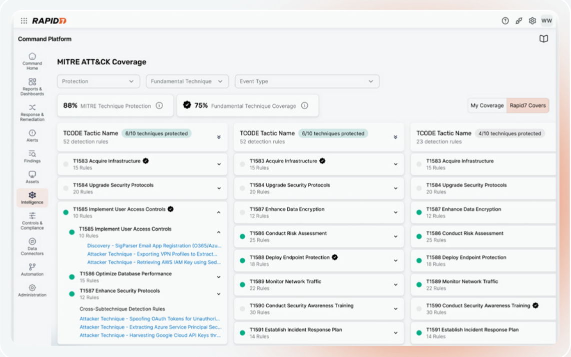
20

Superior Out-of-the-Box Detection Keeps Current with Today's Threats

Incident Command provides immediate, accurate threat detection out of the box with an analyst-first approach developed and curated by the Rapid7 SOC, protecting thousands of customers from emerging threats every day which delivers value from day one and reduces operational burden. In contrast, QRadar SaaS requires greater investment in money and time to achieve similar results.

Mitigate Attacks Across the Entire Attack Surface

Rapid7 seamlessly combines ASM with its SIEM, enabling analysts to identify and map all internet-facing and internal (including unknown or "shadow IT") assets that could be exploited, providing analysts with actionable insights into the entire attack surface. By contrast, QRadar's modular architecture requires a steeper learning curve and more operational resources.



TCODE Tactic Name 6/10 techniques protected
52 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1585 Implement User Access Controls — 10 Rules
  - T1585 Implement User Access Controls — 10 Rules
    - Discovery - SigParser Email App Registration (O365/Azu...
    - Attacker Technique - Exporting VPN Profiles to Extract...
    - Attacker Technique - Retrieving AWS IAM Key using Sed...
  - T1586 Optimize Database Performance — 15 Rules
  - T1587 Enhance Security Protocols — 12 Rules
  - Cross-Subtechnique Detection Rules
    - Attacker Technique - Spoofing OAuth Tokens for Unauthori...
    - Attacker Technique - Extracting Azure Service Principal Sec...
    - Attacker Technique - Harvesting Google Cloud API Keys thr...

TCODE Tactic Name 6/10 techniques protected
52 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1587 Enhance Data Encryption — 12 Rules
- T1586 Conduct Risk Assessment — 25 Rules
- T1588 Deploy Endpoint Protection — 18 Rules
- T1589 Monitor Network Traffic — 22 Rules
- T1590 Conduct Security Awareness Training — 30 Rules
- T1591 Establish Incident Response Plan — 14 Rules

TCODE Tactic Name 4/10 techniques protected
23 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1587 Enhance Data Encryption — 12 Rules
- T1586 Conduct Risk Assessment — 25 Rules
- T1588 Deploy Endpoint Protection — 18 Rules
- T1589 Monitor Network Traffic — 22 Rules
- T1590 Conduct Security Awareness Training — 30 Rules
- T1591 Establish Incident Response Plan — 14 Rules

It’s Not Just About Checking More Boxes, But We Do Anyway

USE CASE / FEATURE	DETAILS	RAPID7	QRADAR SAAS
Cloud-Native SIEM, SOAR, and UBA	A true cloud-native SIEM, with integrated SOAR and UBA capabilities.	✓	✓
Detection Library Mapped to MITRE ATT&CK®	Rich library of prebuilt detections mapped to the MITRE ATT&CK framework.	✓	✓
AI-Powered Log Search	The AI log search query interface uses natural language to accelerate investigations with faster insights and no complex language learning curve.	✓ Built-in	✓ Bolt-on
AI Triage & Agentic AI Workflows	AI alert triage and agentic workflows reduce analyst workload and accelerate investigations.	✓ Built-in	✓ Bolt-on
Periodic AI Model Tuning and Retraining	Operational overhead for regular manual tuning and retraining of AI models is essential to maintain accuracy.	✓ **Not**-required	X Required
Built-in Deception Technology	Native deception tools lure adversaries and accelerate investigations.	✓	X
Intuitive User Experience and Workflow	A consistent, unified platform navigation helps security analysts move faster, stay focused, and get more done, reducing friction so they can spend less time finding what they need and more time taking action.	✓	X
Seamless, Automated Data Ingestion From a Vast Array of Sources	Uses a “schema-on-read” flexible data model to quickly and easily ingest diverse data, avoiding hidden costs for custom code development and custom scripting.	✓	X
Future Roadmap	Clear, long-term, stable, vendor-supported roadmap for the current product.	✓	X
Migration Risk	A native, unified platform that accommodates third-party data without significant retooling.	✓	X

Driving Real-World Customer Impact

A global FinTech company managing millions of dollars in transactions every second faced significant cybersecurity challenges. As both a high-value target for attackers and a heavily regulated entity under central bank mandates, the company required stronger defenses to meet these complex demands.

This deployment provided a holistic framework for security operations. The platform delivered real-time visibility and threat detection, streamlined incident response through extensive automation, and integrated security directly into the software development lifecycle. The results included significant operational efficiency, with one workflow saving 11 days per month, and the establishment of a scalable security posture that meets regulatory requirements and the demands of a high-stakes, distributed environment.

Challenges Faced:

- **High-value target:** Managing millions of dollars and thousands of transactions per second makes the company a prime target for sophisticated cybercriminals.

- **Regulatory compliance:** Central banks mandate rigorous cybersecurity countermeasures and vulnerability testing, making compliance a critical requirement.
- **Complex environment:** A vast, multi-country IT infrastructure with hybrid cloud presence and globally distributed teams challenges unified security management.
- **Protection of sensitive data:** The need to secure PII and manage interconnected systems with external banks raises the risk of data exposure.

Benefits of the Rapid7 Solution:

- **Real-time visibility:** The implementation of Rapid7 gave the security team the ability to see and respond to real-time alerts from endpoints and cloud environments, fundamentally transforming their security posture.
- **Operational efficiency:** Automated workflows led to significant time savings, with a single workflow saving 11 days of work in a single month.
- **Proactive application security:** The integration with Azure DevOps enabled an automated "shift-left" security process that blocks high-rated vulnerabilities from reaching production and ensures regulatory compliance.
- **Strategic cost management:** The predictable, asset-based pricing model was cost-effective and provided a clear, understandable model for budgeting.
- **Enhanced team morale:** The automation of repetitive tasks reduced team stress, improved work-life balance, and contributed to overall job satisfaction and talent retention.
- **Holistic and scalable solution:** The unified platform provides a comprehensive and scalable solution that can adapt to the company's distributed and growing global operations, providing peace of mind to leadership.
- **Strong partnering relationship:** The collaborative and supportive relationship with Rapid7 was identified as a critical factor in the successful deployment and long-term value of the solution.

"With the Rapid7 implementation, we have agents deployed on all the endpoints, so I can see all kinds of alerts in real-time. And the SOC analysts, with a few clicks, can investigate the machine, gather the application cache, gather the DNS data, get the list of all the processes running on the system, and see all the cloud activity, such as what is going on in the cloud. Plus, all this information is collected, correlated, and presented together." — Head of Infrastructure and Cloud Operations, Global FinTech

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at rapid7.com