Death by a Thousand Lows

How Attackers Turn Noise into Full Compromise

Derrick Thomas

CVSS scores the vulnerability. CRSM scores the chain.



Introduction



Derrick Thomas

Deputy Cyber Operations Lead • Deloitte

Cybersecurity leader, former attorney, and educator. I build solutions for clients and frequently break stuff.

TEACHING Adjunct instructor in cybersecurity and IT: St. Petersburg College, Hillsborough Community College, South University

COMMUNITY Co-founder, BSides Tampa • ISC2 Tampa Bay and IAPP Tampa Bay chapters President

CREDENTIALS JD (Stetson Law) • MS • BA (University of Tampa) • CISSP • CISA • CDPSE • CIPP/US • CIPT • CCSK • GMOB

Views expressed are my own and do not represent my employer.

About This Talk

Why chain risk, why now, and what you'll get out of this session.

01

Why Now

CISA's BOD 26-04 (June 2026) moved federal patching from severity alone to exposure, KEV status, exploit automation, and impact. Scoring chains is the next step.

02

Why CRSM

Built after watching the same pattern repeat: teams patched every Critical while attackers walked through a chain of Mediums.

03

What CRSM Is (and Isn't)

An operating model built on inputs you already have: CVSS, EPSS, KEV, MITRE ATT&CK. Not a replacement standard, not a product pitch.

04

What You'll Walk Away With

A working scoring method, two real breach chains, and a Splunk field list you can pilot next quarter.

2026 CORNCON CYBERSECURITY CONFERENCE

Agenda

From vulnerability scoring to attack-path defense.

01 The Problem

Why CVSS alone misses real risk, and how attackers chain findings

02 Introducing CRSM

The model, where it fits, how it scores, and its architecture

03 Real-World Proof

Case studies: Zimbra (2022) and Ivanti EPMM (2025)

04 Operationalizing CRSM

Splunk implementation, weak-signal correlation, dashboards, and limitations

05 Next Steps

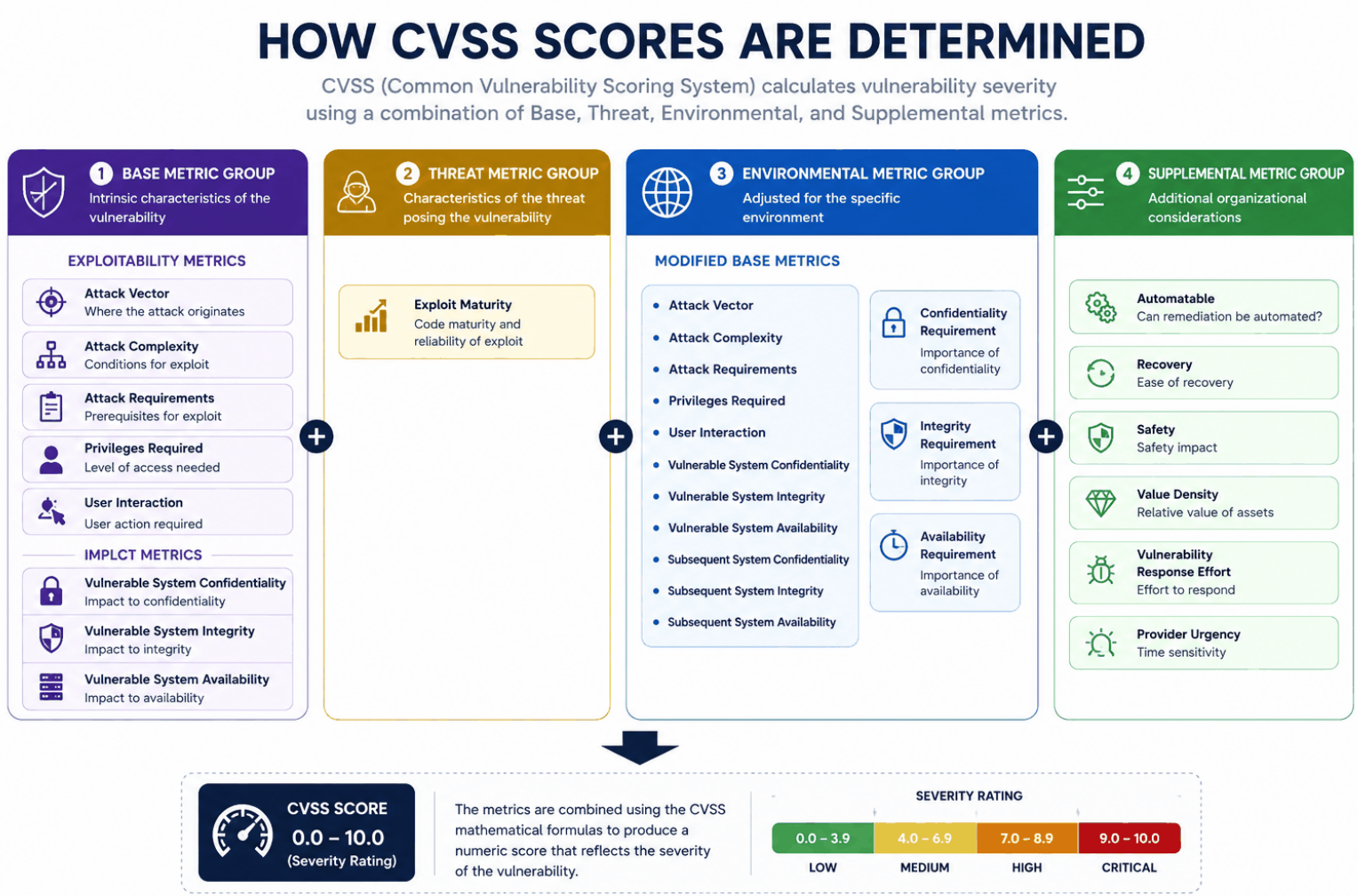
Evaluate fit, scope a pilot, align stakeholders

2026 CORNCON CYBERSECURITY CONFERENCE

What if your biggest risk isn't a Critical CVE?



How CVSS Works



2026 CORNCON CYBERSECURITY CONFERENCE

Attackers Think in Chains



Why Existing Programs Still Fail

- Security tools score findings.
- Attackers exploit relationships.
- CRSM exposes the path between them.



CVSS vs. MITRE ATT&CK vs. CRSM

A simple translation layer for technical leads and senior management.



CRSM does not replace CVSS or MITRE. It connects them into operational risk.

2026 CORNCON CYBERSECURITY CONFERENCE

Where CRSM Fits

You already own tools that touch part of this problem. Here's how CRSM relates to them.

01

Attack Path Graphing (BloodHound, CNAPP path tools)

Strong at mapping identity and cloud paths. CRSM adds vulnerability severity, EPSS/KEV, and business impact into the same score.

02

Exposure Management / CNAPP

Great for cloud-native posture. CRSM is platform-agnostic and pulls in on-prem identity, legacy assets, and SIEM telemetry too.

03

SIEM Correlation & Splunk RBA

Risk-Based Alerting adds up risk per user or host. CRSM scores the ordered attack path and adds vulnerability and business impact inputs.

04

The Honest Positioning

CRSM isn't a tool to replace what you own. It's a scoring layer that sits on top of and connects the tools you already run.

2026 CORNCON CYBERSECURITY CONFERENCE

CISA Confirmed the Problem CRSM Solves



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Directives / BOD 26-04: Prioritizing Security Updates Based on Risk

SHARE:

BINDING OPERATIONAL DIRECTIVES

BOD 26-04: Prioritizing Security Updates Based on Risk

June 10, 2026

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

Map BOD 26-04 to CRSM Scoring

Publicly exposed system → **Exposure**

Known exploited vulnerability → **Vulnerability Severity / KEV**

Automatable exploitation → **Vulnerability Severity / EPSS**

Technical impact → **Identity Risk + Chain Progression**

What is CRSM?

Chain Risk Scoring Model

Traditional vulnerability scoring evaluates weaknesses individually. CRSM evaluates how multiple weaknesses can be chained together by an attacker to create a real compromise path.

Attackers exploit chains, not isolated vulnerabilities.



2026 CORNCON CYBERSECURITY CONFERENCE

CRSM Operating Modes

Use CRSM before exploitation and during active compromise.

A **Pre-exploitation path discovery**

Finds paths attackers could use before they are used: exposed asset + exploitable weakness + privileged access + sensitive data.

B **Active compromise detection**

Finds paths attackers may already be using: suspicious login + lateral movement + privilege use + data access + exfiltration.

Potential Path → Chain Score → Remediation Priority → Active Behavior Escalates → Response Playbook

How CRSM Scores a Chain

Five weighted dimensions combine into a single chain risk score.

Chain Progression
Access → movement → collection → exfiltration



Vulnerability Severity
CVSS, EPSS, KEV, exploit automation



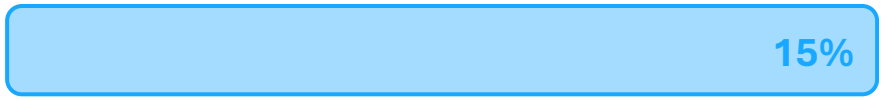
Identity Risk
Privileged, vendor, stale account, service account



Business Impact
Crown jewel asset, sensitive data, operational impact



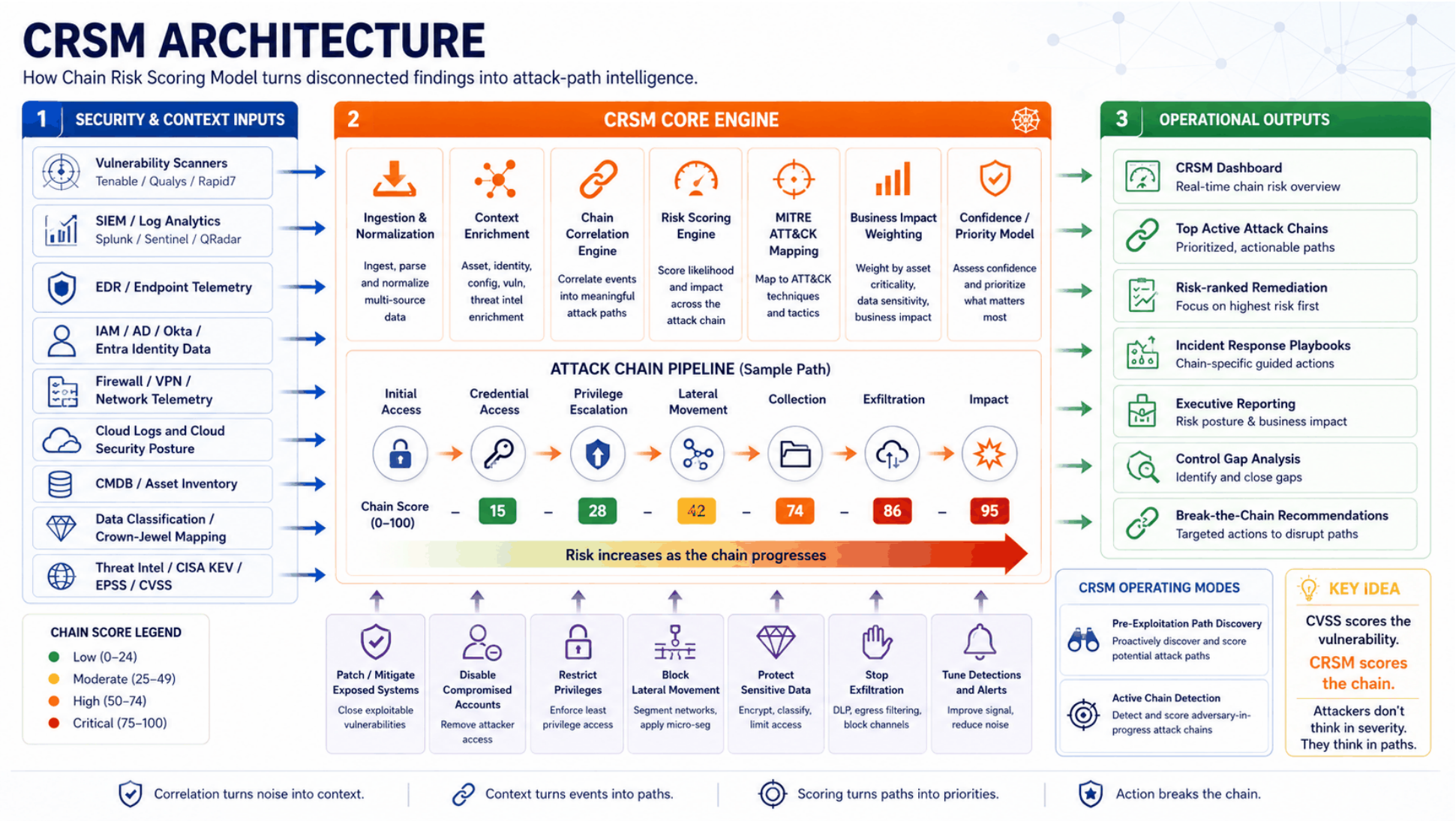
Exposure
Internet-facing, VPN-facing, public cloud path



Medium CVE + Exposed Asset + Privileged Identity + Sensitive Data Path = Critical CRSM Chain

2026 CORNCON CYBERSECURITY CONFERENCE

CRSM Architecture



2026 CORNCON CYBERSECURITY CONFERENCE

Zimbra: Two Flaws, One Breach

The 2022 mass-exploitation chain (CISA AA22-228A), simplified.

01

The Chain

CVE-2022-37042 authentication bypass → CVE-2022-27925 file upload via mboximport. Two CVEs, one unauthenticated path to a web shell.

02

Individually

The file-upload flaw scored High (7.2) and needed admin credentials, so it waited in the queue. The Critical (9.8) bypass wasn't public until mass exploitation was already underway.

03

Chained

More than 1,000 internet-facing Zimbra servers backdoored across government, military, and commercial organizations (Volexity, Aug 2022).

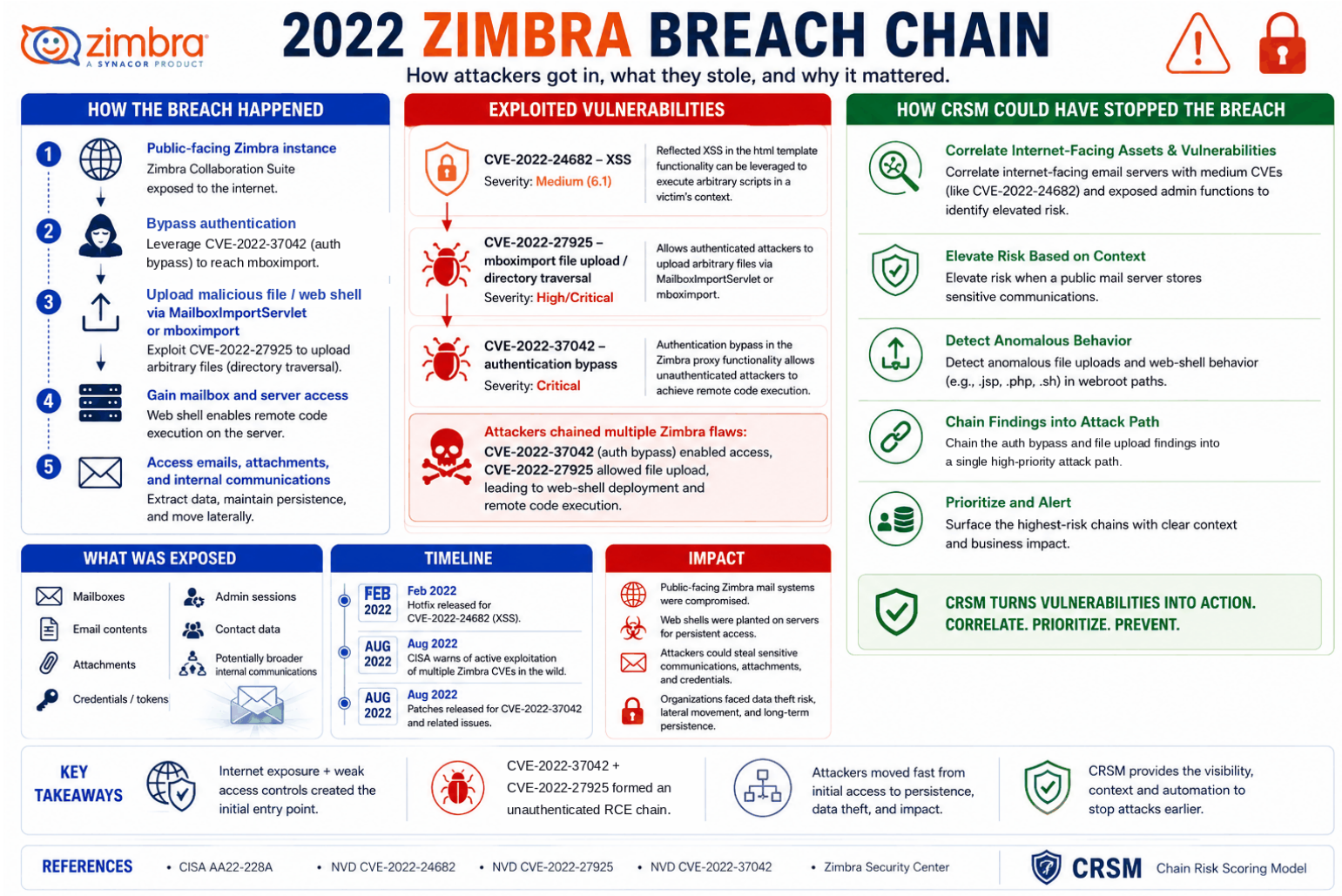
04

Where CRSM Breaks It

A High on internet-facing mail holding privileged mailbox data scores as a critical chain before the bypass exists. Unauthenticated mboximport requests escalate it immediately.

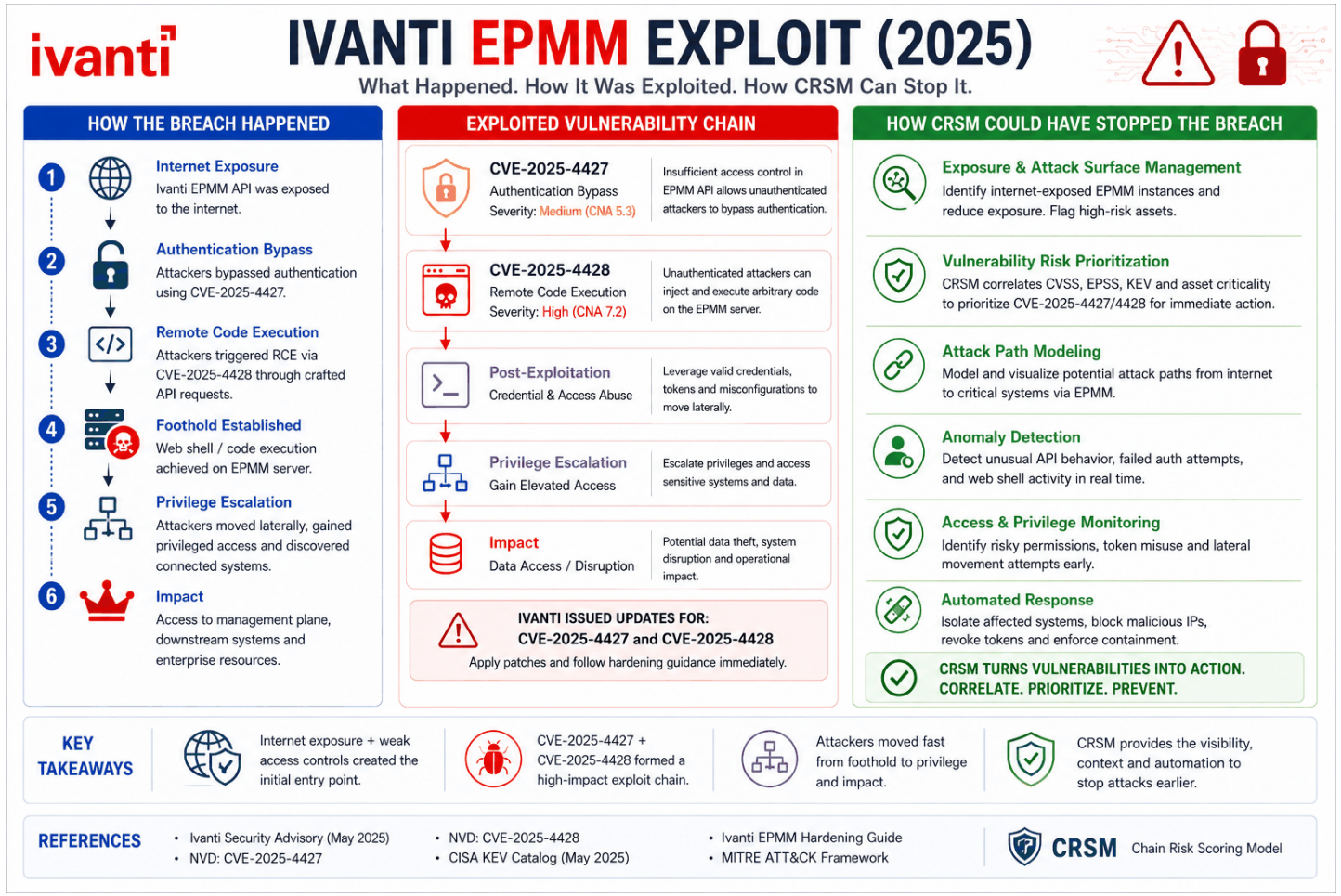
2026 CORNCON CYBERSECURITY CONFERENCE

Zimbra Case Study (Backup)



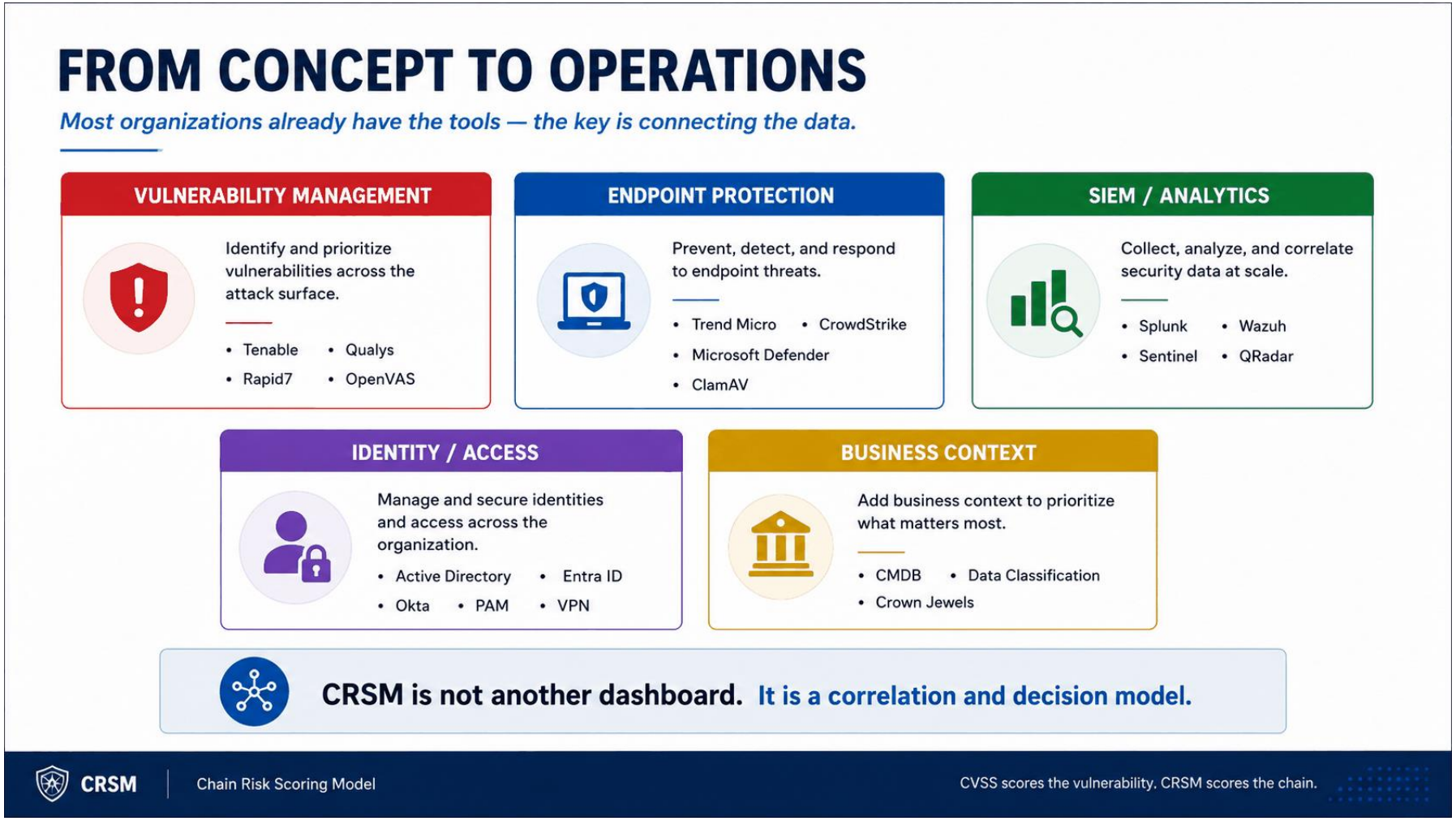
Ivanti Case Study

TIMELINE May 2025: CVEs disclosed & added to KEV → May–Sept 2025: active in-the-wild exploitation → Sept 2025: CISA publishes malware analysis



2026 CORNCON CYBERSECURITY CONFERENCE

Putting CRSM to Work



CRSM & Splunk: Start Here

One CIM extension, ten fields. Full field reference follows as backup.

01

The Spine

crsm_score, chain_id, chain_stage. The three fields every chain event carries.

02

Risk Inputs

asset_criticality, identity_risk, cvss_score, epss_score. What's at stake and how exploitable it is.

03

Exposure & Impact

data_sensitivity, internet_facing, business_impact_score. Whether it's reachable and why it matters.

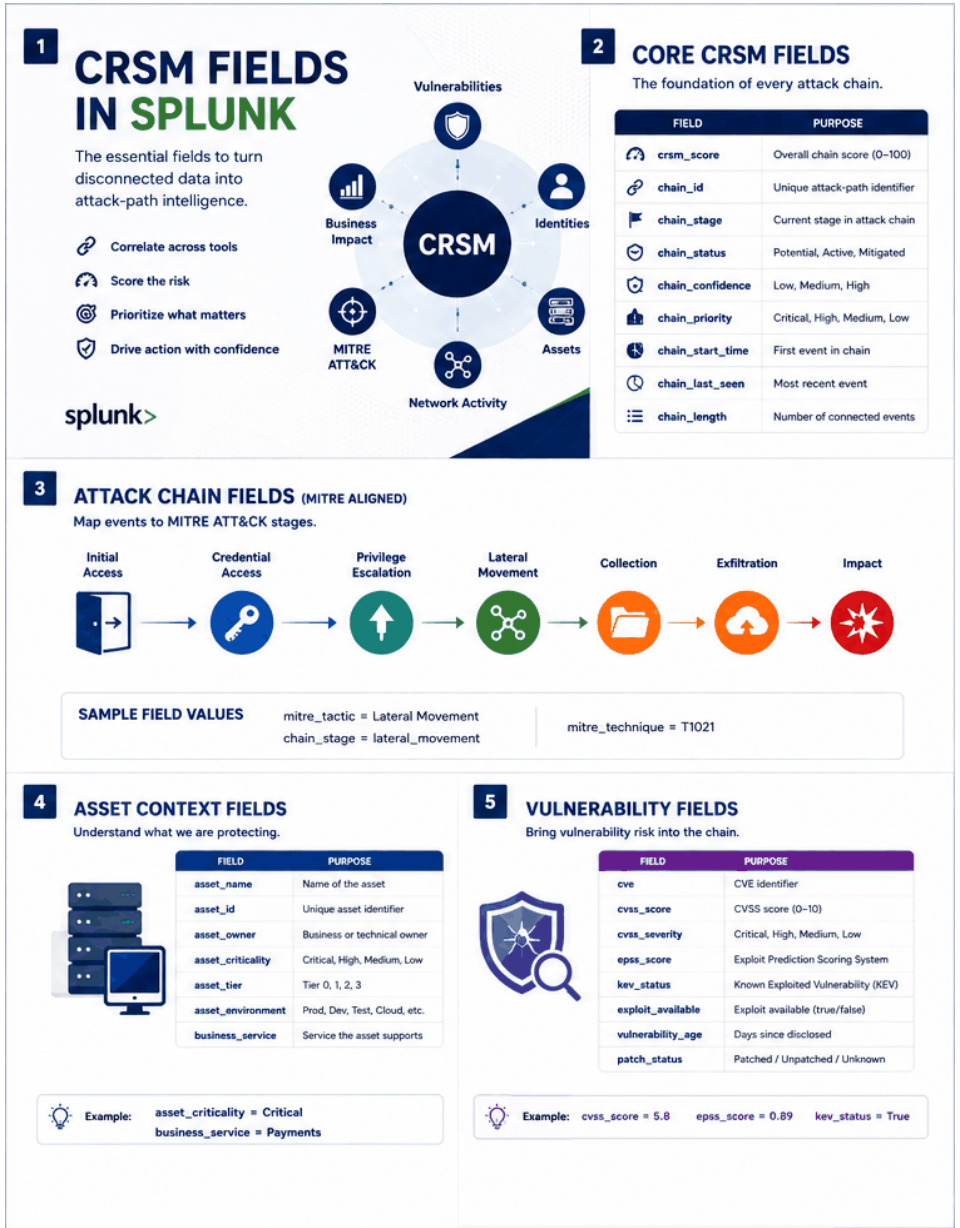
04

What These 10 Power

Dashboards, chain scoring, attack-path analysis, and SOAR playbooks. Everything else is refinement.

2026 CORNCON CYBERSECURITY CONFERENCE

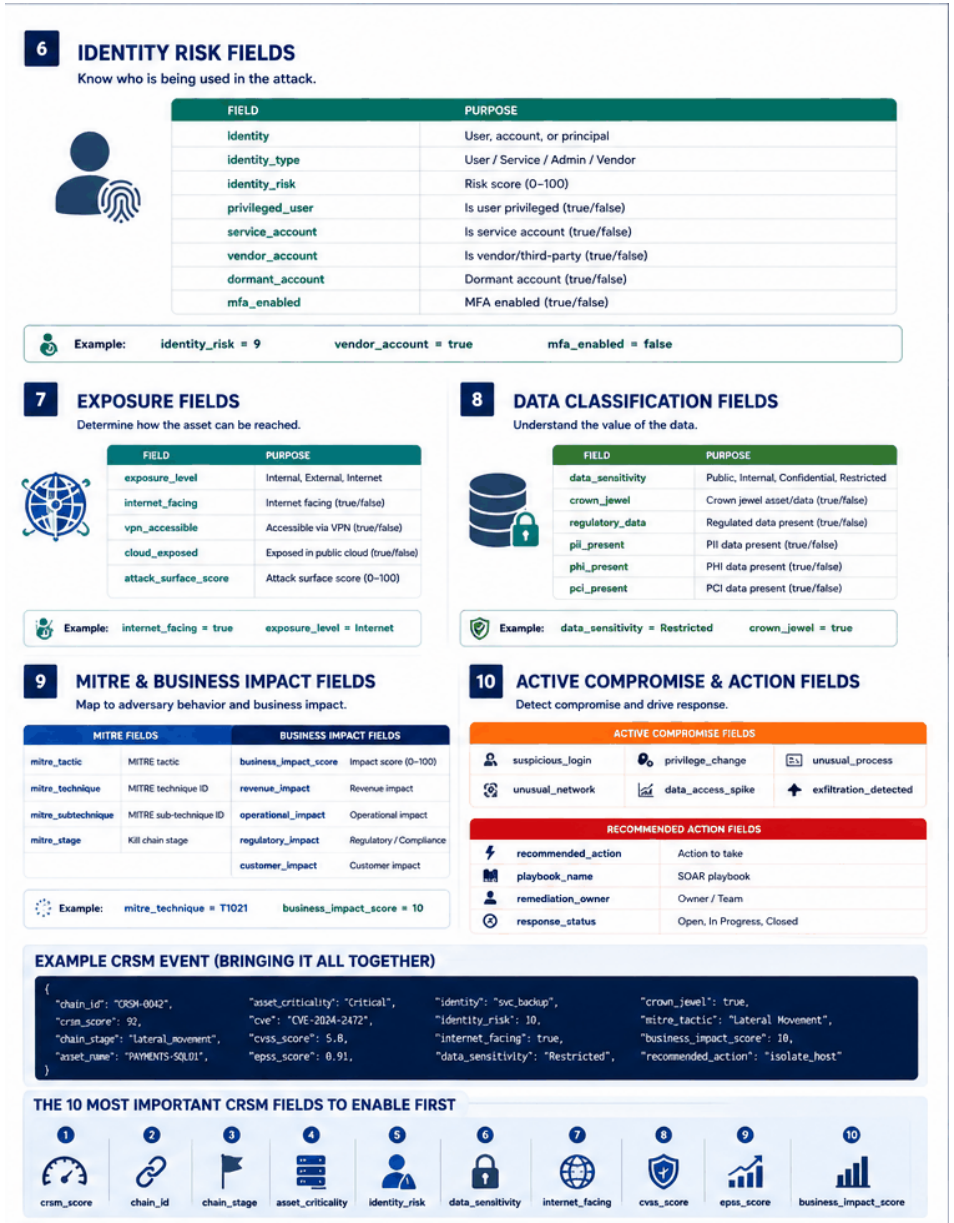
Splunk Fields 1-5 (Backup)



Why a CIM Extension

Not a few bolt-on fields. One CIM extension so Splunk correlates vulnerabilities, identities, assets, network activity, MITRE stages, and business impact into a single attack-path score.

Splunk Fields 6-10 (Backup)



6 IDENTITY RISK FIELDS

Know who is being used in the attack.

FIELD	PURPOSE
identity	User, account, or principal
identity_type	User / Service / Admin / Vendor
identity_risk	Risk score (0–100)
privileged_user	Is user privileged (true/false)
service_account	Is service account (true/false)
vendor_account	Is vendor/third-party (true/false)
dormant_account	Dormant account (true/false)
mfa_enabled	MFA enabled (true/false)

Example: identity_risk = 9 vendor_account = true mfa_enabled = false

7 EXPOSURE FIELDS

Determine how the asset can be reached.

FIELD	PURPOSE
exposure_level	Internal, External, Internet
internet_facing	Internet facing (true/false)
vpn_accessible	Accessible via VPN (true/false)
cloud_exposed	Exposed in public cloud (true/false)
attack_surface_score	Attack surface score (0–100)

Example: internet_facing = true exposure_level = Internet

8 DATA CLASSIFICATION FIELDS

Understand the value of the data.

FIELD	PURPOSE
data_sensitivity	Public, Internal, Confidential, Restricted
crown_jewel	Crown jewel asset/data (true/false)
regulatory_data	Regulated data present (true/false)
pii_present	PII data present (true/false)
phi_present	PHI data present (true/false)
pci_present	PCI data present (true/false)

Example: data_sensitivity = Restricted crown_jewel = true

9 MITRE & BUSINESS IMPACT FIELDS

Map to adversary behavior and business impact.

MITRE FIELDS		BUSINESS IMPACT FIELDS	
mitre_tactic	MITRE tactic	business_impact_score	Impact score (0–100)
mitre_technique	MITRE technique ID	revenue_impact	Revenue impact
mitre_subtechnique	MITRE sub-technique ID	operational_impact	Operational impact
mitre_stage	Kill chain stage	regulatory_impact	Regulatory / Compliance
		customer_impact	Customer impact

Example: mitre_technique = T1021 business_impact_score = 10

10 ACTIVE COMPROMISE & ACTION FIELDS

Detect compromise and drive response.

ACTIVE COMPROMISE FIELDS		
suspicious_login	privilege_change	unusual_process
unusual_network	data_access_spike	exfiltration_detected

RECOMMENDED ACTION FIELDS	
recommended_action	Action to take
playbook_name	SOAR playbook
remediation_owner	Owner / Team
response_status	Open, In Progress, Closed

EXAMPLE CRSM EVENT (BRINGING IT ALL TOGETHER)

```
{
  "chain_id": "CRSM-0042",
  "crsm_score": 92,
  "chain_stage": "lateral_movement",
  "asset_name": "PAYMENTS-SQL01",
  "asset_criticality": "Critical",
  "cve": "CVE-2024-2472",
  "cvss_score": 5.8,
  "epss_score": 0.91,
  "identity": "svc_backup",
  "identity_risk": 10,
  "internet_facing": true,
  "data_sensitivity": "Restricted",
  "crown_jewel": true,
  "mitre_tactic": "Lateral Movement",
  "business_impact_score": 10,
  "recommended_action": "isolate_host"
}
```

THE 10 MOST IMPORTANT CRSM FIELDS TO ENABLE FIRST

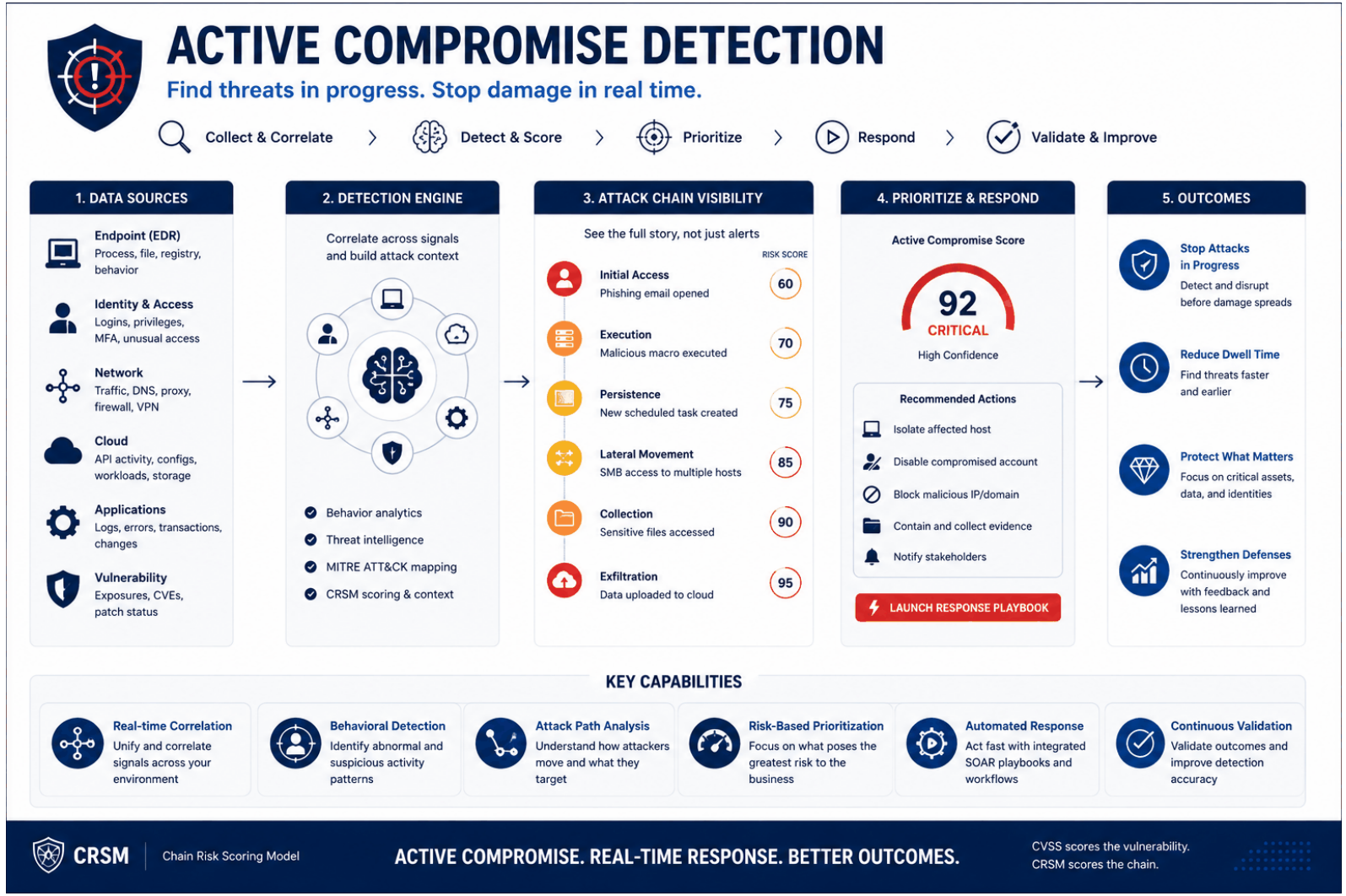
1. crsm_score
2. chain_id
3. chain_stage
4. asset_criticality
5. identity_risk
6. data_sensitivity
7. internet_facing
8. cvss_score
9. epss_score
10. business_impact_score

Start Here: 10 Fields

- crsm_score
- chain_id
- chain_stage
- asset_criticality
- identity_risk
- data_sensitivity
- internet_facing
- cvss_score
- epss_score
- business_impact_score

These ten alone power dashboards, scoring, attack-path analysis, and SOAR playbooks.

Active Compromise Detection



Limitations & Considerations

CRSM is only as good as the practices behind it. Go in with eyes open.

01

Data Quality Dependency

Stale CMDB data or missing asset criticality tags produce a confidently wrong chain score. Garbage in, garbage chained.

02

Tuning & False Positives

Weighting five dimensions means weeks of threshold tuning before chain scores are trustworthy enough to page someone at 2am.

03

Real Integration Lift

The CIM extension needs vulnerability, identity, CMDB, and MITRE data actually flowing into Splunk first. That's a project, not a config change.

04

Not a Replacement for Judgment

A high chain score still needs an analyst to validate before response. CRSM prioritizes attention, it doesn't replace it.

Related Frameworks

Each overlaps part of CRSM. None scores the full chain with business impact.

Framework	What it does	How CRSM differs
Splunk Risk-Based Alerting	Accumulates risk scores per user or host from low-fidelity detections	Scores the ordered path across entities, adds CVSS/EPSS/KEV and business impact
CISA SSVC	Decision tree: exploitation, exposure, automatability, mission impact	SSVC decides one CVE at a time; CRSM scores how CVEs combine
Gartner CTEM	Program model: scope, discover, prioritize, validate, mobilize	CTEM is a process with no formula; CRSM can be its prioritize step
MITRE Attack Flow	Language for describing sequences of ATT&CK techniques	Describes chains but does not score them; pairs with chain_stage
EPSS / KEV / NIST LEV	Exploit probability and evidence of exploitation	Inputs CRSM consumes, not competitors
FAIR	Quantifies risk as loss scenarios in dollars	Translates a CRSM chain into financial exposure for executives

Top 10 Splunk CRSM Use Cases



Executive Dashboard: Key Signals

Illustrative data. The four numbers a stakeholder needs in the first ten seconds. Full view follows as backup.

85
Overall CRSM Score
Critical Risk / 100

14
High-Risk Chains
Active right now

78%
Breach Likelihood
Model estimate

8
Forensic Triage Needed
Assets, this week

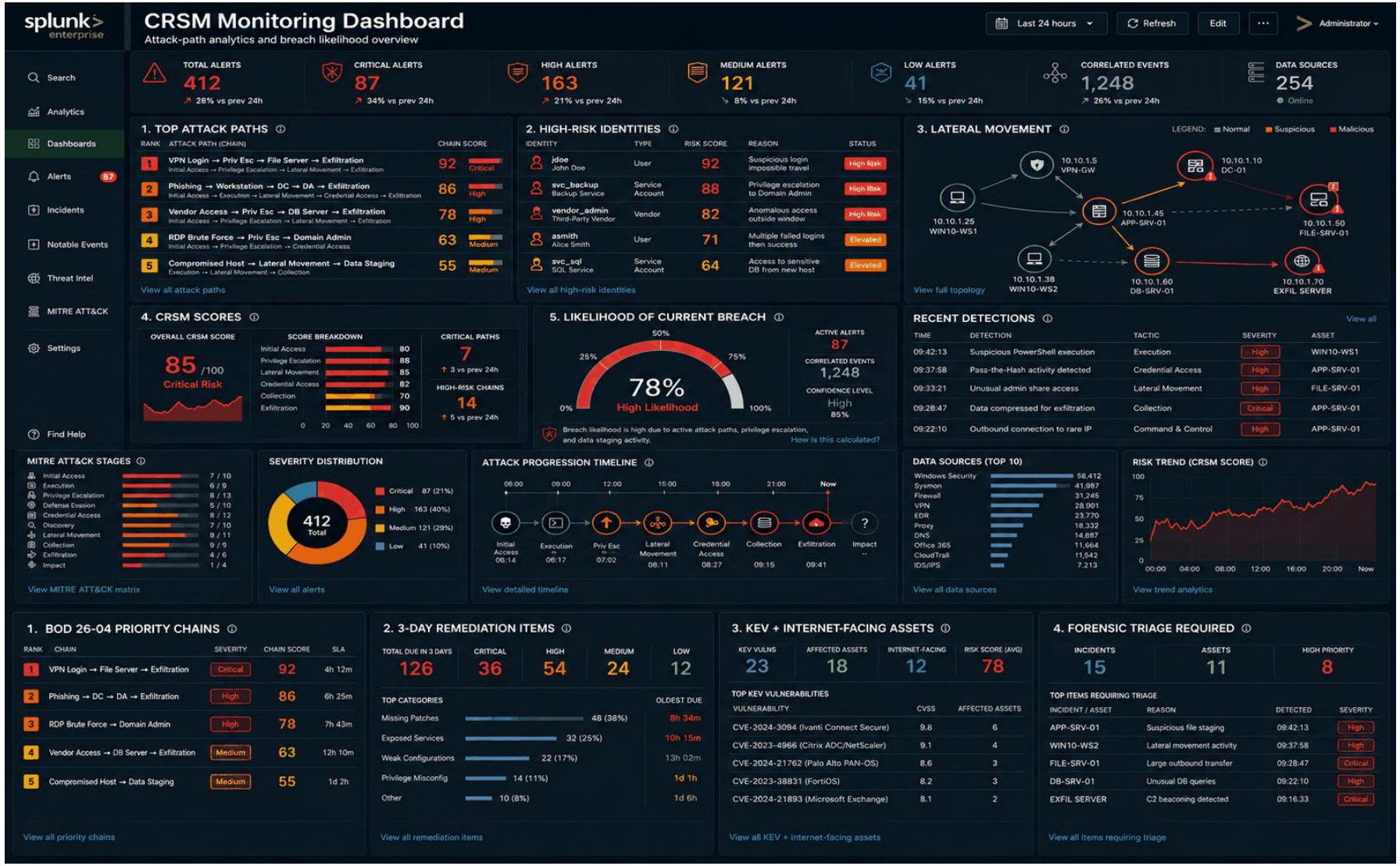
#1 TOP ATTACK PATH **VPN Login → Privilege Escalation → File Server → Exfiltration**

Chain Score 92 • Critical • Up 3 vs. prior 24 hours

Everything below the fold on this dashboard, MITRE stage breakdown, lateral movement graph, top identities, KEV/internet-facing assets, and remediation SLAs, exists to support the four numbers above. The next slide shows that full view for anyone who wants to see it up close.

2026 CORNCON CYBERSECURITY CONFERENCE

Executive Dashboard



2026 CORNCON CYBERSECURITY CONFERENCE

Next Steps

Moving from concept to operational chain-risk defense.

01

Evaluate Fit

Assess how CRSM complements existing vulnerability management, SIEM, and threat intel workflows.

02

Define Pilot Scope

Select a high-value environment or business unit. Map crown jewel assets and known attack paths for initial chain scoring.

03

Align Data Sources

Integrate vulnerability scanners, identity systems, CMDB, and network telemetry into the CRSM scoring pipeline.

04

Measure and Report

Define success metrics, establish executive reporting cadence, and iterate on chain-scoring thresholds based on operational feedback.

2026 CORNCON CYBERSECURITY CONFERENCE

Final Takeaway

Break the path. Stop the breach.



Attackers don’t exploit vulnerabilities.

They exploit paths.

CRSM helps defenders see, score, and break those paths.

CVSS scores the vulnerability. CRSM scores the chain.

Staying secure in an increasingly complex and chaotic world



Let's Continue the Conversation

Take the next step on chain-risk defense.

Want the scoring model or Splunk fields?

DerrickThomas@Outlook.com

www.linkedin.com/in/ddthomas-tampa

Slide deck and CRSM field reference available on request.

Staying secure in an increasingly complex and chaotic world