DVZ community LIVE 2025

18 - 20. MÄRZ 2025
IHK ZU SCHWERIN

DAS MULTI-EVENT FÜR DEN PUBLIC SECTOR

IN MECKLENBURG-VORPOMMERN UND DARÜBER HINAUS

Eine Veranstaltung der

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

DVZ community LIVE 2025

Im Zentrum der Cybersicherheit – das DVZ Security Operations Center

Steffen Schön
Sachgebietsleiter SOC

Agenda

1 **Kurzeinstieg**

2 **Bedrohungslage**

4 **SOC Security Monitoring**

5 **DVZ SOC Mehrwert-Dienste**

Kurzeinstieg

Kurzeinstieg und Eckdaten

- zentrale Protokollierung
- Security Monitoring
- Schwachstellen Prüfung
- Penetrationstests
- Betrieb der Sicherheits-Werkzeuge
- Handlungsempfehlungen
- Alarmierungen

- stetig wachsend


DVZ community
LIVE 2025
Bedrohungslage

Bedrohungslage - eine Rekordhöhe an Gefahren

- Bedrohungslage erreichte im Februar 2025 ein nie dagewesenes Niveau
  - Zuwachs erfolgreicher Angriffe im Februar um 126 Prozent zum Vorjahreszeitraum
  - Deutschland auf Platz 4 der meistangegriffenen Länder
- Anstieg bei Verschlüsselungs-Angriffen (Ransomware)
- Beobachten die Ausnutzung von Hoch-Risiko-Schwachstellen
- Kampagnen werden schneller und wirkungsvoller
- KI gestützte Angriffe revolutionieren die Qualität und Quantität

Bedrohungslage - Angriffsmethoden

- Schadsoftware (Malware)
- Verschlüsselung (Ransomware)
- Daten-Exfiltration
- Überlastungsangriffe (DoS/DDoS)
- Phishing
- Sozial Engineering

Faktor Zeit

- schnelle Angriffe in hoher Qualität können Schutzmechanismen überfordern
  - Updates / Sicherheitslücken
  - Fehlkonfiguration und Härtung
  - alte Verfahren
  - Nutzeranfälligkeit
- Risiko jedoch stetig gegeben, besonders bei End-Nutzern oder Internet-Komponenten
- Angriffsziel: vollständige Kompromittierung
- Nutzerarbeitsplatz verschlüsselt?

  -> eher Glück als Unglück

Ablauf von Angriffen in großen Umgebungen

Stunden
- Infektion / initialer Zugang
- schlagartig und häufig unauffällig

Tage
- Einnistung / Rechteerweiterung
- über Tage / Wochen

Wochen
- Ausbreitung / Daten Exfiltration
- über Wochen / Monate

Monate
- Verschlüsselung und Erpressung
- schlagartig

repeat
- Lösegeldzahlung?
- Wiederinfektion bei 50 % der Unternehmen innerhalb von 12 Monaten

DVZ community LIVE 2025

SOC - Security Monitoring

Lessons learned aus Cyberangriffen

Minuten	• Infektion / initialer Zugang • schlagartig und häufig unauffällig	← Analyse der Bedrohungslage (Alarme, Angriffswellen, …)
Tage	• Einnistung / Rechteerweiterung • über Tage / Wochen	← Detektion und Spuren (Kommando- und Kontrollserver, Konten-Aktivitäten, …)
Wochen	• Ausbreitung / Daten Exfiltration • über Wochen / Monate	← Detektion und Spuren (Verbindungs-daten, Zugriffsversuche, …)
Monate	• Verschlüsselung und Erpressung • schlagartig	← Detektion und Spuren (Leistungsdaten / Datenänderungen, …)
repeat	• Lösegeldzahlung? • Wiederinfektion bei 50 % der Unternehmen innerhalb von 12 Monaten	

Sicherheitsereignisse sichtbar machen

Protokollschichten identifizieren, anbinden und interpretierbar machen

- Netzwerk
- Hypervisor
- Container Cluster
- Betriebssysteme
- Services
- Sicherheitssysteme
- Endpunkte

Aufbau von Protokoll-Daten generell unterschiedlich

Tools und Werkzeuge

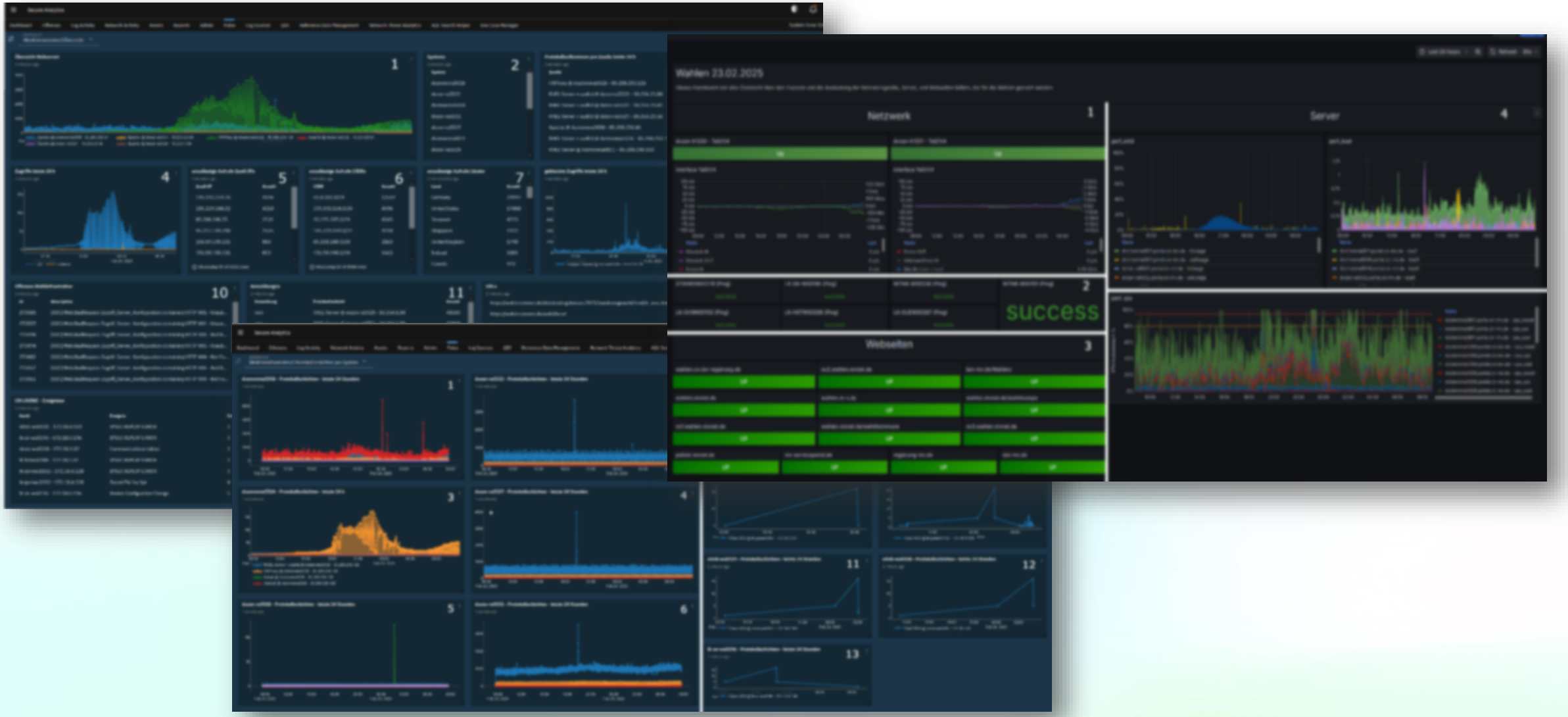
Kern: SIEM

- zentrale Protokollierung
- Normalisierung relevanter Protokolldaten
- Prüfung über Alarmierungs-Regelwerke
- Interpretation sekundärer Ereignisse
- Netzwerk-Flow-Daten
- Baselining
- Alarme
- Dashboards
- Reports
- Automatisierung

JSA Juniper Secure Analytics (JSA) / IBM QRadar
Elastic Stack (Elasticsearch, Kibana & Logstash)
Tenable Security Center / Tenable Nessus

DVZ community LIVE 2025

Darstellung und Benachrichtigung

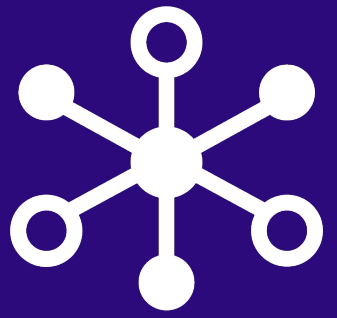


DVZ Security Operations Center (SOC)

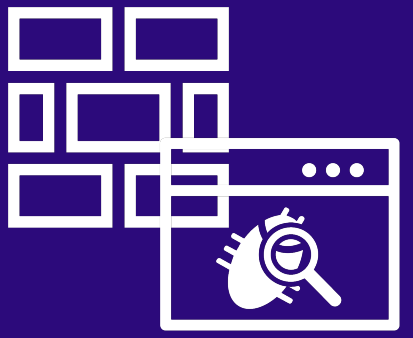
DVZ SOC – Mehrwert-Dienste

Mehrwertdienste SOC

Härtungs-
Tests



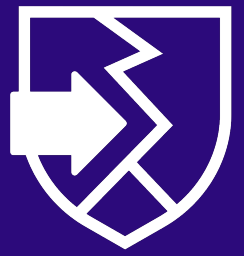
CN LAVINE



sekundäre
Sicherheits-
Ereignisse

Internet

Schwachstellen-
Scans



Penetrations-
Tests

Infrastruktur-
Ereignisse /
Fachverfahren

DVZ SOC

Alarme
24/7

Reports

DVZ community LIVE 2025

DVZ Security Operations Center (SOC)

Steffen Schön

s.schoen@dvz-mv.de

0385 4800 373