ThreatConnect.

The ThreatConnect Museum of CYBER DEFENSE PAST & FUTURE

TIMELINE OF CYBER DEFENSE

Fossils of the Past
(EARLY 21ST CENTURY)

Security teams had no centralized way to track adversaries, relying on raw logs, manual investigations, and isolated expertise to detect threats.

TECHNOLOGY

Log Managers & SIEMs

Introduced centralized logging and correlation, helping security teams analyze threats.

While many SIEMs survive today, it's through symbiotic relationships with newer technologies like TIPs and SOARs.

EVOLUTIONARY PRESSURES

The Alert Swamp

Overwhelming data volumes - without context or prioritization - drowned analysts in an ocean of logs.

Fig 1. The Alert Swamp

COMMON THREATS OF THE ERA

Worm Epidemic

Rise of early Nation-State threats like China's APT-1

The Dawn of Threat Intelligence
(2010s)

Analysts struggled to keep up with threat intelligence feeds, needing a way to aggregate and standardize data.

TECHNOLOGY

Threat Intelligence Platforms (TIPs)

Provided a single place to collect threat intelligence, helping teams organize external and internal intelligence.

EVOLUTIONARY PRESSURES

Gathering intelligence is one thing - acting on it is another. Without automation and prioritization, intelligence platforms were little more than filing cabinets for threats.

Some TIPs underwent rapid and destructive mutations, producing chimeric abominations that claimed to be SIEMs, TIPs, XDRs, and UEBAs all in one. Unable to find an ecological niche, they soon died out.

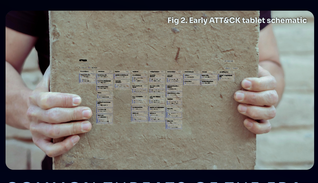

Fig 2. Early ATT&CK tablet schematic

COMMON THREATS OF THE ERA

Ransomware strains like Cryptolocker emerge

High Profile APT attacks like Fancy Bear & Lazarus Group

The Age of Invention & Discovery
(PRESENT DAY)

Security teams needed faster response to threats but lacked efficient workflows to manage incidents and orchestrate actions.

TECHNOLOGY

SOAR (Security Orchestration Automation & Response)

Introduced playbook-driven automation to speed up response times.

Threat Intelligence Operations

An evolutionary leap in the right direction: the large braincase of the threat intelligence platform with the speed and agility of a SOAR.

EVOLUTIONARY PRESSURES

While automation increased overall efficiency, and the union of automation and intelligence increased overall effectiveness, cyber defense teams continued to struggle to focus on the most impactful threats.

Fig 3. Developments in automation

COMMON THREATS OF THE ERA

Cloud takeovers like TeamTNT

Ransomware

While each leap forward helped teams overcome the challenges of the past, many still remain: high burnout and team turnover, alert fatigue, low confidence in response and detection, and disconnects between business and cyber defense priorities mean that a quantum leap is needed.

The Intel Hub & Cyber Defense's Next Era
(THE FUTURE)

Expanding Attack Surface, Attack Complexity, and AI adoption give adversaries an exponential advantage. Meanwhile, Defensive Capacity is growing linearly. Unable to solve exponential problems with linear evolution, many cybersecurity solutions have gone extinct. They lacked the context and priorities to act decisively.

TECHNOLOGY

The Intel Hub: Threat & Risk-Informed Defense

- Prioritize defenses based on business risk
- Contextualize intelligence in alignment with those priorities
- Act decisively on those threats and adapt your priorities based on outcomes

COMMON THREATS OF THE ERA

AI-powered cybercrime

Supply chain attacks

Ransomware-as-a-service